セキュリティプロトコルの一貫性および正常終了一致の同一参加者による複数セッションを考慮した検証法

根岸和義[†,††] 米崎直樹[††]

従来のセキュリティプロトコルの検証では，(1) すり替えられることなくメッセージを伝達する，(2) 秘密を保持する，ことの 2 点を検証することが一般的である．ただし，この中で考慮される攻撃のパターンでは，同一参加者の複数セッション間におけるプロトコルの，同一部分メッセージどうしのすり替えが考慮されていなかった．本論文ではこのような攻撃を考慮した一貫性の検証方法を与え，さらに，そこで用いられる推論規則の健全性を証明した．一方，電子商取引において，第三者の攻撃があっても，プロトコルを実行する 2 つのプロセスが，同期して正常終了する必要がある．そこで，セッションを構成するプロセスの間で正常終了の判断が一致するようなプロトコルになっているか否かを検証する方法を提案し，適用例を示した．

Verification Method for Consistency and Normal Termination Agreement on Multiple Sessions with the Same Principals in a Security Protocol

Kazuyoshi Negishi[†,††] and Naoki Yonezaki[††]

Generally verification of security protocols has focused on the subjects, (1) transmission of the messages without replacement, and (2) secret maintenance of messages. The pattern of attack considered in these researches does not take the following situation into account, that is the case where the replacement of messages might be done between the different sessions of a protocol. We give verification rules for consistency that take account of these attacks. We also verify the soundness of the verification rule. In electronic commerce trading, protocol must be executed between two processes and terminate normally under attacks by the malicious principals. We propose the method to verify the agreement of the decision of normal termination for processes which consist the session. Finally, we show the effectiveness of our methods by applying it to the example of ITU X.509 protocol.

1. まえがき

インターネットを利用した電子商取引の普及にともない，通信のセキュリティを守ることによる不正防止の必要性が高まっている．通信のセキュリティを守るためには，個別のメッセージのセキュリティを守るための暗号化の技術は必須であるが，それだけでは十分ではない．メッセージのすり替えなどの攻撃によりプロトコルの実行中にセキュリティが破られることがある．このような攻撃に耐性のあるプロトコル（セキュリティプロトコル）の技術が必要とされる．本論文では，悪意を持つ攻撃者（イントルーダ）の存在を前提として，セキュリティプロトコルの検証に関して検討する．

従来のセキュリティプロトコルの検証法の研究としては，代数的モデルに対する状態生成と解析（モデルチェック）によるもの[1)]，論理によるプロトコル解析を行う BAN 論理[2)]，これを拡張して型によるメッセージのすり替えの可能性検出を行う SG 論理[3)] などの論理によるものがあった．また，BAN 論理による自動解析ツールの研究も行われている[4)]．さらに，BAN 論理をセキュリティではなく一般のネットワークプロトコルの完全性の検証に用いる研究も行われている[5)]．BAN 論理に対しては，並行するセッションを利用した攻撃に対処できないとの批判があり[6)~8)]，メッセージの型チェックによるすり替えの可能性検出を提案している SG 論理もこの問題を解決できていない．これら，論理による考察ではプロトコルの定義をもとに問

† 株式会社日立製作所ビジネスソリューション開発本部
Business Solution Systems Development Division, Hitachi Ltd.
†† 東京工業大学大学院情報理工学研究科計算工学専攻
Department of Computer Science, Graduate School of Information Science and Engeneering, Tokyo Institute of Technology

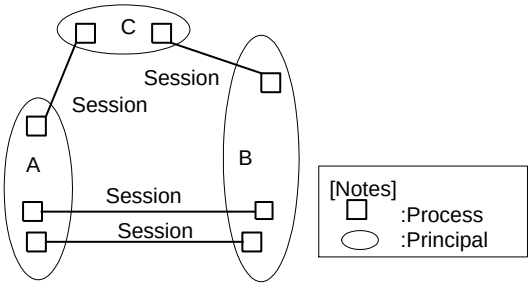

図 1 参加者，プロセスとセッション
Fig. 1 Principals, processes and sessions.

題となりそうなメッセージを選択し，これらメッセージに関して個別に検証を行うのが通例であった．

我々の想定するプロトコルの実行環境のモデルを**図 1** に示す．プロトコルは確定した参加者をともなったプロセスにより実行される．プロトコルの 1 回の実行をセッションと呼ぶ．各プロセスは 1 度に 1 つのセッションを実行する．同一参加者の異なるプロセスはセッションを並行して実行することができる．

本論文では，セキュリティプロトコルの目的を，電子商取引への適用を前提として，下記の 2 項目とし，イントルーダの攻撃により，これらの目的が達成できない可能性を検証する．

プロトコルの一貫した実行 プロトコルを実行し，正常終了したプロセスがセッションの最初から最後まで同一の定められた相手のプロセスからのメッセージのみを受信し，他のセッションからメッセージとすり替えられたりしない．

正常終了の一致 あるセッションでプロトコルを実行している複数のプロセスのうち 1 つがセッションを正常に終了したと判断するならば，残りのプロセスも同一の判断を下す．

なお，セキュリティプロトコルの目的の 1 つである秘密の保持に関しては，本論文の検討範囲外とし，別の手段により保持されているものとする．秘密情報，特に参加者の秘密キー，共用キーがイントルーダに知られることはないと仮定する．

本論文の 2 章では，制約条件，用語定義を述べる．3 章では，プロトコルのモデルとその初期条件を示し，4 章ではプロトコルの目的を定義し，5 章では論理式による検証の手順を示すとともにその正しさを証明する．6 章では適用例を示す．

2. 前提条件と用語

2.1 前 提 条 件

プロトコル

- 扱うプロトコルは 1 種類のみとする．
- プロトコルは 2 人の参加者の間の通信を定義する．また，これら 2 人の参加者は役割を逆にすることはない．
- プロトコルは 2 人の参加者の交互の通信手順であり，プロトコルの流れは途中で分岐しない．
- プロトコルはイントルーダの攻撃のない場合，正しく動作する．たとえば，保持していないメッセージを送信したりせず，キーは適切な参加者に配布されている．
- プロトコルで送信されるメッセージは，セッションの参加者以外の参加者の名前やキーを含まない．受信者の名前やキーが含まれているならそれを宛先を表す情報と解釈する．
- プロトコルは，相手の秘密キーで電子署名されたメッセージを受信してそれを再度相手に送信するなど，自分が内容を知らないメッセージを送信することはないものとする．
- プロトコルでは，暗号化メッセージを受信した後，そのキーを受信して復号化することはないものとする．

セッション

- セッションはプロトコルの一連の実行である．
- セッションは並行して複数同時実行可能である．
- セッション間でメッセージの受け渡しはない．
- セッション中で使用されるすべてのメッセージはセッションの開始時に与えられる．

参加者

- 正規の参加者はプロトコルに従い，不正をしない．また，プロトコルの送受信で想定されている内容，他の参加者の初期状態を知っている．
- メッセージ固有の特性（共用キーなど）は，初期状態で保持しているものはその時点，受信したものなら受信した時点で参加者に分かる．
- セキュリティを守るために可能な限り受け取ったメッセージが想定されている内容か否かのチェックを行う．

暗号

- メッセージは暗号化キーにより暗号化したメッ

セージに変換され，復号化キーによりこの逆の変換がなされる．2 種類のキーが同一の場合（共用キー）と，異なる場合（公開キーと秘密キー）がある．秘密キーで暗号化したメッセージを電子署名されたメッセージと呼ぶ．

- 暗号化メッセージは完全で，キーなしでは解読できない．
- 暗号化メッセージと同じものを偶然に作ることはできない．
- 暗号化メッセージの集合からキーを推定することはできない．

イントルーダとその攻撃

- イントルーダは自分の秘密キーと，参加者の公開キー以外のキーは持っていない．
- 送受信されたメッセージはすべて傍受できるとする．
- 正規の参加者の送信するメッセージを傍受，改変，または横取りすることができる（ただし，暗号化されたメッセージはキーがなければ復号や改変はできない）．
- 正規の参加者になりすまして，偽造，あるいは過去に傍受したメッセージを送信することができる（知らないキーで暗号化されたメッセージは偽造できない）．

2.2 用　　語

以下の説明と論理式中で用いられる用語を定義する．

2.2.1 参加者，プロセスおよびその状態

(1) 参加者

参加者は以下のいずれかである．

A，B，C： 特定の参加者を表す定数．

p，q： 参加者を表す変数．

以後，P，Q を参加者を表すメタ変数として用いる．

(2) プロセス

P が参加者であるとき，P^k で参加者 P が実行するセッション k のプロセスを表す．また，$S^k_{P_i}$ で参加者 P が実行するセッション k のプロセスの i 番目の状態を表す．

ただし，単一のセッションに関することが明らかな場合は，k を省略する．

2.2.2 メッセージ

(1) アトミックメッセージ

アトミックメッセージとは，参加者を表す定数，あるいは，以下のいずれかである．

$M, M_1, M_2, \ldots$： 単なるデータを表す定数．

$N, N_1, N_2, \ldots$： nonce（必要に応じて生成される，過去に使用されたことのないデータ）を表す定数．

$K, K_1, K_2, \ldots$： キーを表す定数．

x, x_1, x_2： アトミックメッセージを表す変数．

アトミックメッセージには下記のように参加者の情報を付加することができる．

M_{jP}： 参加者 P が初期値として持つ単なるデータを表す定数．

N_{jP}： 上記の nonce を表す定数．

K_{jPQ}： 参加者 P と Q の共用キーを表す定数．

K_{jP}： 参加者 P の公開キーを表す定数．

K^{-1}_{jP}： 参加者 P の秘密キーを表す定数．

ここで，$j = 0, 1, 2, \ldots$ であり，$j = 0$ の場合は省略する．アトミックメッセージの集合を **Atom** で表す．

(2) メッセージ

メッセージは以下のように帰納的に定義される．

- アトミックメッセージはメッセージである．
- X_1 と X_2 がメッセージならばそれらの連接 X_1, X_2 もメッセージである．
- X がメツセージ，Z がキーならば X を Z で暗号化した $\{X\}_Z$ もメツセージである．

また，以降では，X_j をメッセージを表すメタ変数として，Z_j をキーを表すメタ変数として用いる．$inv(Z_j)$:Z_j の逆キーを表す関数とする．（$inv(K_{jP}) = K^{-1}_{jP}$，$inv(K^{-1}_{jP}) = K_{jP}$ かつ $inv(K_{jPQ}) = K_{jPQ}$）ここで，$j = 0, 1, 2, \ldots$ であり，$j = 0$ の場合は省略する．

2.2.3 タグ付きメッセージ

受信したメッセージ中，および初期値として保持しているメッセージ中の同一のアトミックメッセージの，複数の出現を区別するために，アトミックメッセージ（たとえば M_{1P}）の右肩にタグ w を付加したタグ付きアトミックメッセージ（M^w_{1P}）を考える．ここで，タグ w の値を以下のように定義する．

$w = iu$： i 番目の送受信されるひとまとまりのメッセージの中で，u 番目に出現するアトミックメッセージである．

$w = 0$： 各参加者が最初から保持しているアトミックメッセージである．

送受信に出現するメッセージおよび初期値として保持しているメッセージ X_j について，その中で出現するアトミックメッセージにすべてタグを付加したものをタグ付きメッセージとよび，$\bar{X}_j$ で表す．ここで，$\bar{X}_j$ のタグ $tag(\bar{X}_j)$ の値は，すべてのアトミックメッセージのタグを結合したものとして定義される．X_j の異

なる出現については，そのタグの値は異なることがあるため，異なるタグの値を持つ同一のメッセージを区別するために，$\bar{X}_j, \bar{X}_j{}'$ なる記法を用いることがある．また，キー Z_j に対して，タグ付きのキーを $\bar{Z}_j$ で表す．さらに，タグ付きのアトミックメッセージを表す変数を $\bar{x}$，$\bar{x_1}$，$\bar{x_2}$ とする．また，メッセージに対応するタグの値は，たとえば，$tag(\{M^{12}_{1A}, N^{13}_{2B}\}_{K^{14}_{3AB}}) = 121314$ である．メッセージに付けられたタグからそのメッセージか何番目の送受信メッセージであるか，あるいは初期値であるかを定める関数 $st(w)$ を下記のように定義する．

- $w = iu_1iu_2 \ldots iu_m$ の場合 $st(w) = i$
- $w = 0$ の場合 $st(w) = 0$

i 番目に送受信されるひとまとまりのタグ付きメッセージを定数 U_i で表す．

2.2.4 メッセージのタイプ

アトミックメッセージ X には，あらかじめタイプ $Type(X)$ が定義されている．$Type_P(X)$ は P が X の部分メッセージについて判定可能な型を可能な限り付加したメッセージ X の型である．ただし，X に含まれる暗号化メッセージで，P がそれを解読するキーを持たない場合その型は □ となる．

$$Type_P(X_1, X_2) = Type_P(X_1), Type_P(X_2)$$

$$Type_P(\{X\}_Z) = \begin{cases} \{Type_P(X)\}_{Type_P(Z)} \\ \cdots P\ has\ \overline{inv(Z)}\text{が導けるとき} \\ \square \\ \cdots P\ has\ \overline{inv(Z)}\text{が導けないとき} \end{cases}$$

$$Type_P(X) = Type(X) \quad \cdots X \in \mathbf{Atom}$$

$P\ has\ \bar{Z}$ は後述の論理式であり，P が $\bar{Z}$ を持っていることを表す．

3. プロトコルのモデルと初期条件

3.1 プロトコルの送受信と参加者の状態

プロトコルのモデルにおける $1 \sim n$ 番目の送受信のうち，i 番目の送受信を下記のように記述する．

$$i : P \rightarrow Q : U_i$$

このとき，P^k の状態は U_i の送信時に S^k_{Pi-1} から S^k_{Pi} に遷移し，Q^k の状態は U_i の受信時に S^k_{Qi-1} から S^k_{Qi} に遷移する．これらは必ずしも同時ではない．また，セッション k の開始時の参加者のプロセス P^k の状態は S^k_{P0} である．

3.2 メッセージ集合と役割

P が初期メッセージ集合として保持するアトミックメッセージの集合を $Init(P)$ とする．

セッションごとに異なる値（セッション固有値と呼ぶ）が生成されるアトミックメッセージの集合を **Session** とする．セッションをまたがって共通な，または，セッションごとに生成されるが異なる保証のないアトミックメッセージの集合を **Com** とする．

セッションの参加者の集合を **Prin**，セッションのすべてのタグ付きアトミックメッセージの集合を **TagAM** とする．

4. セキュリティプロトコルの目的

ここでは，セキュリティプロトコルの目的として以下を取り扱う．

4.1 メッセージの伝達を一貫性を保って行う

相手に伝えるべきアトミックメッセージの集合を **Share** とする．このとき，一貫性のある伝達とは，セッションを構成するプロセスは，すべての $X \in$ **Share** につき，すべて相手に伝達され，セッションを構成する他のプロセスからのみ X を受信し，X に関するすり替えがあればそれを検知できることをいう．

4.2 セッション正常または異常終了の判断の一致

セッション k を実行するプロセス P^k，Q^k は最後の 2 個のメッセージ U_{n-1}，U_n の送受信により**図 2** のように状態が遷移する．U_{n-1} の伝達がイントルーダにより妨害されて，Q^k に伝わらない場合は，P^k，Q^k はそれぞれ状態 S^k_{Pn-1}，S^k_{Qn-2} にとどまり，時間がたてばセッションは異常終了し双方の判断に不一致はない．U_n の伝達がイントルーダにより妨害されて，P^k に伝わらない場合は，P^k，Q^k はそれぞれ状態 S^k_{Pn-1}，S^k_{Qn} にとどまり，P^k はセッションが異常終了，Q^k はセッションが正常終了したと判断する．このような判断の不一致を単純なメッセージの伝達のみで防止することはできない．判断の一致が必須であるオンラインシステムなどでは，2 フェーズコミットプロトコルにより，この問題を解決している[9]．しか

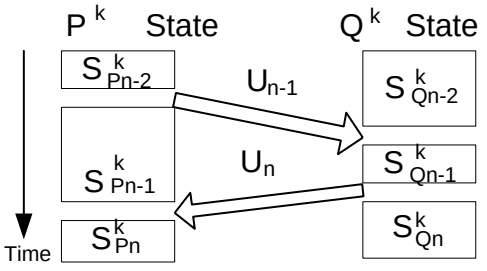

図 2 プロセスの最終状態遷移
Fig. 2 Final stage of the transitions of the processes.

し，通常，実際のプロトコルでは最後のメッセージに関してメッセージの消失の可能性のある場合は，受信側が送信側に問い合わせて，判断することで，送信側との食い違いを防止している．本論文においても，最後のメッセージに関しては，このような補助的な手段があるものとする．

U_{n-1}，U_n が送信されていないのにイントルーダが代理で送信することができ，受信者がこれを見破れないとき，送信者の状態が進んでいない場合でも，受信者の状態が進んでしまう．これを防止するには U_{n-1}，U_n の中にイントルーダには作成できない情報が入っている必要がある．このように，U_{n-1}，U_n を本来の相手から受信したことが保証できれば，互いに相手の状態が最終状態まで進むことが保証される．

5. 論理による検証

前章の 2 つの目的を達成していることを検証するために，以下の形式言語を用いる．

5.1 論 理 式

本論文で使用する論理式は以下に定義される基本命題を古典的論理結合子 $(\wedge, \vee)$ で拡張し，さらに参加者とメッセージ変数に関する全象束縛と存在束縛を加えたものである．以下の基本命題式の記述方法は，BAN 論理のものを使用した．最初の 7 個の論理式は BAN 論理におけるものと同じである．ただし，タグ付きのメッセージを含む論理式は，特定の出現場所のメッセージに関する論理式であり，これは本論文で導入された．

(1) $P \models \varphi(X)$：P は持っているメッセージ X について，論理式 φ を信じる．論理式 φ には，$\models$ は含まれない．
(2) $P \lhd \bar{X}$：P は $\bar{X}$ を受け取る．
(3) $P \overset{Z}{\leftrightarrow} Q$：$Z$ は P と Q の共用キーである．P，Q 以外は Z を知らない．
(4) $\overset{Z}{\mapsto} P$：Z は P の公開キーである．P 以外は $inv(Z)$ を知らない．
(5) $P\,has\,\bar{X}$：P は $\bar{X}$ を持っている．
(6) $P \vdash \bar{X}\,to\,Q$：P はかって Q に $\bar{X}$ と言ったことがあり，Q は $\bar{X}$ を受け取った☆．
(7) $P\,says\,\bar{X}\,to\,Q$：P から Q へセッション内でメッセージ $\bar{X}$ を送受信する．そこで送られるメッセージ $\bar{X}$ は，他のセッションの同一送受信における，同一部分メッセージとのすり替えを除き，その送受信の中で改変されない☆,☆☆．
(8) $\bar{X}_1\,in\,\bar{X}_2$：$\bar{X}_1$ は $\bar{X}_2$ の構成要素．
(9) $unforged X$：X はアトミックメッセージであって，イントルーダにより改変されていない．
(10) $auf\ X$：（almost unforged）X はアトミックメッセージであって，他のセッションの同一送受信における同一部分メッセージとのすり替えを除き，改変されていない．
(11) $\bar{X}\,isto\,P$：$\bar{X}$ は宛先 P の情報を含むメッセージである．
(12) $replaceunit\bar{X}$：$\bar{X}$ は 1 つの通信の途中で，イントルーダによりそのメッセージをすり替えられる可能性がある．しかし，イントルーダにより，$\bar{X}$ の部分メッセージがその部分のみ，すり替えられることはない．
(13) $unreplaceable\,\bar{X}$：受信した $\bar{X}$ は他のセッションの同一送受信における同一部分メッセージとのすり替えを除き，すり替えられる可能性がない．
(14) $guard_Q\,\bar{X}_1\bar{X}_2$：$\bar{X}_1$ と $\bar{X}_2$ は暗号化または電子署名によりイントルーダが更新できない同一のメッセージ（ガードされたメッセージ）の一部として送信され，Q に受信される．
(15) $onetoonecon\,\bar{X}_1\bar{X}_2\bar{X}_2'$：$guard_Q\,\bar{X}_1\bar{X}_2$ が成立するような **Session** の要素 $\bar{X}_1\bar{X}_2$ において，X_1 はメッセージの受信者 Q の初期メッセージ集合の要素であり，X_2 は送信者 P $(\neq Q)$ の初期メッセージ集合の要素である．また，この送受信の後，Q から P へ，ガードされたメッセージの一部として，$\bar{X}_2'$ が返信される．
(16) $X_1 \sim_P X_2$：X_1 と X_2 は同一のガードされたメッセージの一部として送信され P に受信される．
(17) $X \in \mathbf{Set}$：X が集合 **Set** の要素である．
(18) $X \notin \mathbf{Set}$：X が集合 **Set** の要素ではない．

5.2 前提となる論理式

プロトコルの初期条件から以下のように，前提となる論理式を定義する．

- $X \in Init(P)$ ならば，$Phas\bar{X}$ ただし，$tag(\bar{X}) = 0$，かつ $P \models unforged\,X$ である．
- $i : P \to Q : U_i$ ならば $Q \lhd U_i$ である．
- $K_{jPQ} \in Init(P)$ ならば，$P \models P \overset{K_{jPQ}}{\leftrightarrow} Q$ である．

☆ $to\,Q$ は本論文で拡張した部分であり，メッセージ $\bar{X}$ の送り先が Q であることを確認していることを表す．

☆☆ 同一部分とのすり替えに関する部分は，本論文で拡張した部分である．

- $K_{jP}^{-1} \in Init(P)$ かつ $K_{jP} \in Init(Q)$ ならば $Q \models \overset{K_{jP}}{\mapsto} P$ である．

ここで，3 番目の論理式は，前提条件のプロトコルの項において，キーの配置が適切に行われることから定義される．また，4 番目の論理式は，これに加えて，参加者の項の他の参加者の初期状態を知っていることから定義される．

5.3 メッセージの伝達

メッセージの確実な伝達の推論は以下の手順で行われる．本節の論理による検証のうち，5.3.3 項までは，BAN 論理と記述方式の違いはあるが同等の内容であるため，推論のあらすじのみを示し，ここで省略した推論規則は付録に採録した．

5.3.1 メッセージを送信したことがある

P と Q しか知りえない共用キー Z で暗号化されたメッセージは，Q が作って送信したものである．異なる参加者ペア間のメッセージとすり替えられたなら，それを正しいメッセージと信じることはない．

$$\frac{P \lhd \overline{\{X\}_Z} \wedge P \models Q \overset{Z}{\leftrightarrow} P}{P \models Q \mid\sim \bar{X}\, to\, P}$$

同様にして，相手にしか作れない電子署名されたメッセージ $\bar{X}$ があり，$\bar{X}$ の中にあて先を表す情報を含む（isto）場合，以下の推論規則が使用される．

$$\frac{P \models \bar{X}\, isto\, P \wedge P \models \overset{inv(Z)}{\mapsto} Q \wedge P \lhd \overline{\{X\}_Z}}{P \models Q \mid\sim \bar{X}\, to\, P}$$

5.3.2 メッセージのすり替え

イントルーダが作成することのできない部分メッセージ $\bar{X}$ 全体の，同一の参加者ペア間の他の部分メッセージとのすり替えは，$\bar{X}$ の受信者を Q としたとき，同一の型 $Type_Q(X)$ のメッセージが，プロトコルの他の部分に存在しなければ不可能である．メッセージ $\bar{X}$ についてこのような部分が存在しないことを $unreplaceable\, \bar{X}$ で表す．このような X に関する推論規則は下記である．

(1) まず，送受信されるひとかたまりのメッセージの中で，イントルーダが自由に更新可能な部分メッセージ X を $changeable\, \bar{X}$ とする．

$$\frac{changeable\, \overline{X_1, X_2}}{changeable\, \bar{X}_1}$$

$$\frac{changeable\, \overline{\{X\}_{K_{jP}}}}{changeable\, \bar{X}}$$

$$\overline{changeable\, U_i}$$

(2) 次に $changeable \bar{X}$ であるが，イントルーダが作り替えることができないものを $replaceunit\, \bar{X}$ という．

$$\frac{changeable\, \overline{\{X\}_{K_{jPQ}}}}{replaceunit\, \overline{\{X\}_{K_{jPQ}}}}$$

$$\frac{changeable\, \overline{\{X\}_{K_{jP}^{-1}}}}{replaceunit\, \overline{\{X\}_{K_{jP}^{-1}}}}$$

(3) $replaceunit\, \bar{X}$ のうちで，他の部分とのすり替えができない部分を $unreplaceable\, \bar{X}$ とする．

$$\frac{replaceunit\, \bar{X} \wedge Sametype(\bar{X}) = \phi}{unreplaceable\, \bar{X}}$$

$$\frac{unreplaceable\, \bar{X} \wedge \bar{X}_1\, in\, \bar{X}}{unreplaceable\, \bar{X}_1}$$

ここで，関数 $Sametype(\bar{X})$ は下記のように，$\bar{X}$ と同じ型のタグ付きメッセージの集合として定義される．

$$\begin{aligned} Sametype(\bar{X}) = \{\bar{X}_1 \mid\ & \bar{X}\, in\, U_i \wedge Q \lhd U_i \wedge \\ & (Type_Q(X_1) = Type_Q(X)) \wedge \\ & tag(\bar{X}_1) \neq tag(\bar{X})\} \end{aligned}$$

5.3.3 すり替えなく伝達

他のセッションの同一部分とのすり替えを除き，メッセージがすり替えられず，相手の参加者に伝達されることを確実な伝達と呼び，その十分条件を表す推論規則が以下のように定義される．

$$\frac{P \models Q \mid\sim \bar{X}\, to\, P \wedge unreplaceable\, \bar{X}}{P \models Q\, says\, \bar{X}\, to\, P}$$

$$\frac{\begin{array}{c} P \models Q\, says\, \bar{X}\, to\, P \wedge \\ X \in Init(Q) \wedge X \notin Init(P) \end{array}}{P \models auf\, X}$$

5.3.4 メッセージの一貫性を保った伝達

同一参加者が他のセッションのプロセスで送信した同一部分のメッセージとのすり替えのないことの検証を以下の推論規則により行う．まず，X_1 と X_2 が P から Q へ同時に確実な伝送によって伝えられることを表す論理式 $guard_Q\, \bar{X}_1\bar{X}_2$ を下記の推論規則の結論とする．

$$\frac{\bar{X}_1\, in\, \bar{X} \wedge \bar{X}_2\, in\, \bar{X} \wedge Q \models P\, says\, \bar{X}\, to\, Q}{guard_Q\, \bar{X}_1\bar{X}_2}$$

さらに $guard_Q\, \bar{X}_1\bar{X}_2$ が成立する P から Q へ同時に伝えられるメッセージ X_1 と X_2 がそれぞれ異なる参加者 Q，P が同一部分のすり替えを除いて相手に伝達したアトミックメッセージであり，かつ **Session** の要素である場合に，この送信が相手に到着すれば，互いに相手の初期メッセージ集合の要素であり **Session** の要素であるアトミックメッセージを共有することに

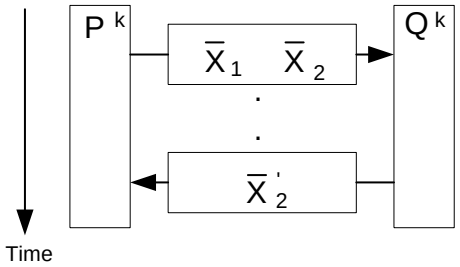

図 3 1 組のプロセスによるセッション固有値の共有
Fig. 3 Sharing the session parameters by a pair of processes.

なる．

図 3☆に示すように，上記伝達の後で，Q から P へ P の初期値である $\bar{X_2}'$ が確実な伝達で返される場合，上記の送信が相手に到着したことが確認される．上記の送受信は P^k，Q^k 以外には送信や受信ができず，他のプロセスがセッション k の X_1 や X_2 を保有していても，それ以後の状態に進むことはできない．このような伝達が存在することを $onetoonecon\ \bar{X_1}\bar{X_2}\bar{X_2}'$ と記述する．そこで，以下の推論規則を導入することができる．

$$\frac{\begin{array}{r} guard_Q\ \bar{X_1}\bar{X_2} \wedge \\ X_1 \in \mathbf{Session} \wedge X_2 \in \mathbf{Session} \wedge \\ P \models auf\ X_1 \wedge Q \models auf\ X_2 \wedge \\ st(tag(\bar{X_2})) < st(tag(\bar{X_2}')) \wedge \\ P \models Q\ says\ \bar{X_2}'\ to\ P \end{array}}{onetoonecon\ \bar{X_1}\bar{X_2}\bar{X_2}'}$$

この規則の健全性は以下のように証明される．

定理 1 $onetoonecon\ \bar{X_1}\bar{X_2}\bar{X_2}'$ が推論されたなら，このプロトコルに基づいたすべてのセッションにおいて，$st(tag(\bar{X_2}'))$ 番目の状態以降は，イントルーダのいかなる攻撃のもとでも，そのセッションの固有値である X_1 と X_2 をともに持つプロセスは 1 組のみであり，その他のプロセスは X_1 と X_2 のいずれも持たない．

証明

$\bar{X_1}, \bar{X_2}$ の送信と，$\bar{X_2}'$ の送信をそれぞれ

$$i : P \rightarrow Q : U_i \quad \text{および} \quad j : Q \rightarrow P; U_j$$

とする．ここで，$onetoonecon\ \bar{X_1}\bar{X_2}\bar{X_2'}$ が推論されたと仮定する．すると，これを証明する規則は上記の規則のみであるから，前提である $Q \models auf\ X_1$，$P \models auf\ X_2$ が成立する．さらに，$Q \models auf\ X_1$，$P \models auf\ X_2$ を証明する規則は 1 個のみであり，その前提条件である $X_1 \in Init(Q)$，$X_2 \in Init(P)$ がそれぞれ成立している．ここで，セッション k を考え，プロセス P^k，Q^k の初期値として X_1^k，X_2^k をそれぞれ与える．またここで，本証明ではセッション k の X_1 を X_1^k と，$\bar{X_1}$ を ${\bar{X_1}}^k$ と表す．プロセス P^k が U_i を Q^k に送る．もし，Q^k がイントルーダの攻撃によりこの U_i を受け取らず，かわりに $P^{k'}$ の送信した ${\bar{X_1}}^k\ in\ U_i'$ なる U_i' を受け取っていたとすると，P^k 以外のプロセス $P^{k'}$ は，X_2^k を含む送信を行わないから，Q^k は ${\bar{X_2}'}^k$ を含む U_j を返すことができない．また，Q^k 以外の $Q^{k''}$ は，${\bar{X_1}}^k\ in\ U_i$ なる U_i を X_1^k が自分の持っているセッション固有値 $X_1^{k''}$ と異なるので，正常な相手プロセス以外からの通信であることが分かるから受け取らない．したがって，何かを受け取るとすれば U_i とは異なる $X_1^{k''}\ in\ U_i''$ なる U_i'' を受け取っている．このとき，${\bar{X_2}}^{k''}\ in\ U_i''$，$X_2^{k''} \neq X_2^k$（$X_2^k$ を U_i から取り出して U_i'' に入れることはできない）より，$Q^{k''}$ も P^k に ${\bar{X_2}}^k\ in\ U_j$ なる U_j を送り返すことができない．したがって，U_j が返ってきたということは，U_i が Q^k に受け取られたということを表す．このとき，Q^k，P^k はともに X_1^k と X_2^k を持つ．

また，状態 $S_{Qi}^{k'''}$ 以前で，イントルーダの介入により X_2^k を持つに至った $Q^{k'''}(\neq Q^k)$ が存在するとしても，X_2^k と $X_1^{k'''}$ を含む U_i''' を送信するプロセスが存在しないため，処理を状態 $S_{Qi}^{k'''}$ 以降に進めることができない．

さらに，状態 $S_{Pj}^{k''''}$ 以前で，同様にして X_1^k を持つ $P^{k''''}(\neq P^k)$ は処理を状態 $S_{Pj}^{k''''}$ 以降に進めることはできない．なぜなら，先ほどと同様の理由により，$P^{k''''}$ の送信した U_i''''（X_1^k および $X_2^{k''''}$ を含む）を Q^k が受信して返信しない限り，$X_2^{k''''}$ を含む返信はありえず，$P^{k''''}$ は状態 $S_{Pj}^{k''''}$ に進むことができないからである．もし，Q^k が受信した場合には処理が継続できるが，この場合は $P^{k''''}$ がすなわち P^k の役割を果たしていることになる．

したがって，状態 S_{Pj}^k 以降で，X_1^k，X_2^k の両方を持つプロセスは P^k，Q^k のみであり，その他のプロセスは X_1^k，X_2^k のいずれも持たない． **証明終わり**

$guard$ を用いて，Q がメッセージ X_1 と X_2 を渡される場合の関係 $\sim_Q$ を下記のように定義する．

$$\frac{\begin{array}{r} Q \models auf\ X_1 \wedge Q \models auf\ X_2 \wedge X_1 \in \mathbf{Session} \wedge \\ X_2 \in \mathbf{Session} \wedge guard_Q\ \bar{X_1}\bar{X_2} \end{array}}{X_1 \sim_Q X_2}$$

関係 $\sim_Q$ に関して対称律が成り立つ．さらに，この

☆ メッセージは暗号化または電子署名によりガードされているものとする．

関係 $\sim_Q$ に対し下記の推移律を定義する．

$$\frac{(X_1 \sim_Q X_2) \wedge (X_2 \sim_Q X_3)}{X_1 \sim_Q X_3}$$

このような関係を用いて，さらに以下の性質を推論することができる．

- すべての q の初期値でないセッション固有のメッセージ x は関係 $\sim_q$ を用いてグループ分けしたとき，同じグループに属する．

$$\forall q \in \mathbf{Prin}[\forall x_1, x_2 \in (\mathbf{Session} - Init(q)) \; [x_1 \sim_q x_2]] \quad (1)$$

ここで，変数のドメインが有限集合 $\{t_1, \ldots, t_m\}$ であるような全象束縛と存在束縛に関して，下記の推論規則を導入する．

$$\frac{\varphi[t_1/y] \wedge \ldots \wedge \varphi[t_m/y]}{\forall y \in \{t_1, \ldots, t_m\}[\varphi]} \qquad \frac{\varphi[t_i/y]}{\exists y \in \{t_1, \ldots, t_m\}[\varphi]}$$

ただし，φ は論理式，$\varphi[t/y]$ は論理式 φ の中の変数 y の自由出現を t で置き換えることを表す．

- セッションが 1 組のプロセスだけで成立していることを保証するため，少なくとも 1 つの $onetoonecon$ が推論される必要がある．

$$\exists \bar{x_1}, \bar{x_2}, \bar{x_2}' \in \mathbf{TagAM} \; [onetoonecon\, \bar{x_1}\bar{x_2}\bar{x_2}'] \quad (2)$$

これらを用いて，$Q \models auf\, X$ を満たすメッセージが，同一部分のすり替えもない条件は，少なくとも 1 つの $X_1 \in \mathbf{Session}$ かつ P の初期値である X_1 と同一のガードされたメッセージで相手の参加者から送信され，同一部分とのすり替えのないことを表す下記により定義される．

$$\frac{(Q \models auf\, X_1) \wedge (X_1 \in \mathbf{Session}) \wedge (guard_Q\, \bar{X_1}\bar{X}) \wedge Q \models auf\, X \wedge \text{式 (1)} \wedge \text{式 (2)}}{Q \models unforged\, X}$$

5.3.5 伝達すべきメッセージの一貫性保持

伝達すべきメッセージ（**Share**）を一貫性を保って伝えている（初期値として持たない側の参加者で，$unforged$ となる）かの検証は，以下の式により行われる．

$$\forall x \in \mathbf{Share}[\exists p, q \in \mathbf{Prin}[x \in Init(p) \wedge q \models unforged\, x \wedge q \in (\mathbf{Prin} - \{p\})]] \quad (3)$$

5.4 正常終了に関する参加者の判断の一致

セッションの最後の 2 回の送受信を，

$$n-1 : p \rightarrow q : U_{n-1}$$
$$n : q \rightarrow p : U_n$$

としたときに，参加者 p，q の判断が一致するための条件は，U_{n-1} と U_n にイントルーダが偽造できない情報が入っていることであり，その条件は下記である．

$$\exists p, q \in \mathbf{Prin}[\exists \bar{x_1}, \bar{x_2} \in \mathbf{TagAM}[x_1 \in \mathbf{Session} \wedge x_2 \in \mathbf{Session} \wedge q \models p\; says\; \bar{x_1}\; to\; q \wedge \bar{x_1}\; in\; U_{n-1} \wedge p \models q\; says\; \bar{x_2}\; to\; p \wedge \bar{x_2}\; in\; U_n]] \quad (4)$$

上記の条件（式 (3)，式 (4)）をすべて検証することにより，セキュアなプロトコルがその目的を達成しているかどうかを検証することができる．

6. 適 用 例

本論文の検証方式を下記の ITU X.509 プロトコル[10] に適用して，そのセキュリティプロトコルとしての目的達成を検証する．本例のプロトコルはメッセージのセキュリティを保った伝送に関する基本手順を定める標準である．本標準のドラフトに対して文献 2) で攻撃の可能性が示されているが，ここに示す標準[10] では，対策済みである．

$$1 : A \rightarrow B : \quad A^{11}, \{N_{1A}^{12}, N_{2A}^{13}, B^{14}, M_{1A}^{15}, \{M_{2A}^{16}\}_{K_B^{17}}\}_{K_A^{-118}}$$
$$2 : B \rightarrow A : \; B^{21}, \{N_{3B}^{22}, N_{4B}^{23}, A^{24}, N_{2A}^{25}, M_{3B}^{26}, \{M_{4B}^{27}\}_{K_A^{28}}\}_{K_B^{-129}}$$
$$3 : A \rightarrow B : \quad A^{31}, \{N_{4B}^{32}, B^{33}\}_{K_A^{-134}}$$

その他の初期条件は下記のとおりである．

$$Init(A) = \{N_{jA}, M_{jA}, A, B, K_A, K_B, K_A^{-1}\}$$
$$Init(B) = \{N_{j'B}, M_{j'B}, A, B, K_A, K_B, K_B^{-1}\}$$
$$\mathbf{Com} = \{M_{jA}, M_{j'B}, A, B, K_A, K_B, K_A^{-1}, K_B^{-1}\}$$
$$\mathbf{Session} = \{N_{jA}, N_{j'B}\}$$
$$\mathbf{Share} = \{M_{jA}, M_{j'B}\}$$
$$\mathbf{Prin} = \{A, B\}$$
$$\mathbf{TagAM} = \{N_{1A}^0, N_{1A}^{12}, \ldots, K_B^{-10}, K_B^{-129}\}$$
$$Type(N_{jA}) = Type(N_{j'B}) = Non$$
$$Type(M_{jA}) = Type(M_{j'B}) = Msg$$
$$Type(A) = Type(B) = ID$$
$$Type(K_A) = Type(K_B) = Key$$
$$Type(K_A^{-1}) = Type(K_B^{-1}) = Key$$

ここで，$j = 1\; or\; 2$ かつ $j' = 3\; or\; 4$ である．

この前提条件のもとで論理による検証を行う．まず，すり替えの可能性の検証であるが，U_1，U_2，U_3 はいずれも送信者の秘密キーにより電子署名されており，かつ受信者を識別する情報が電子署名内部に含まれており，異なる参加者ペアのセッションとのすり替えの可能性はない．また，この 3 個の送受信は含むメッセージの数が異なっていることから，別の部分と互い

にすり替えを行うことはできない．

同一参加者ペア間の同一部分とのすり替えについて検討する．A と B の両方のセッション固有値を含む送受信は 2 番目の U_2 のみである．U_2 内のメッセージに関しては，たとえば $guard_A\ N_{4B}^{23}N_{2A}^{25}$ である．これに対して，N_{4B}^{32} が 3 番目のメッセージ U_3 に含まれるから，$onetoonecon\ N_{2A}^{25}N_{4B}^{23}N_{4B}^{32}$ が推論される．したがって，式 (2) が推論できる．また，$N_{1A} \sim_B N_{2A} \sim_B M_{1A} \sim_B M_{2A}$ および $N_{3B} \sim_A N_{4B} \sim_A M_{3B} \sim_A M_{4B}$ より，式 (1) が推論できる．さらに，$P \models auf\ X$ が成立するのは，N_{1A}, N_{2A}, N_{3B}, N_{4B}, M_{1A}, M_{2A}, M_{3B}, M_{4B} である．これらはそのまま $unforged$ となる．

ここで，以下の 2 つの性質を検証する．

(1) 一貫性を保ったメッセージの伝達：**Share** の要素はすべて，初期値として持っていない方の参加者で $unforged$ となっているので，式 (3) が推論できる．

(2) 終了に関する参加者の判断の一致：2 番目および 3 番目（最後）の送受信において，ガードされた伝達が行われており，各々有効な **Session** の要素を含むことから，式 (4) が推論できる．

7. まとめ

セキュリティプロトコルの検証方法として，従来考慮されていなかった並行するプロセス間でのプロトコルの同一部分どうしのすり替え，および正常終了判断の一致について，下記を示した．

(1) 暗号や電子署名によりイントルーダが更新できない（ガードされている）メッセージによりプロセスの固有値を伝達することで，プロセス A^1, B^1 間でのみこれらのプロセス固有値を持つ条件として，プロセス A^1 からプロセス B^1 へ A^1 と B^1 のプロセス固有値を同時に送り，そのあと A^1 のプロセス固有値を返送すれば十分であることを証明し，それを推論規則として与えた．

(2) プロセス間で正常終了の判断を一致させる方策として最後の 2 個のメッセージに前述のガードされたメッセージが挿入されていればよいことを示した．

時間に関してシリアルなセッションを利用した攻撃に加えて，並行したセッションを利用した攻撃，特に同一部分のすり替えの可能性の検証方法を提案した．このことはモデルチェックによっても検証が可能であるが，本方式によればすべての状態を作り出すことなく，より少ない計算により検証が可能である．

セキュリティプロトコルの例として ITU 国際標準の X.509 に本論文の検証方式を適用しその効果を実証した．

謝辞 本研究の機会を与えていただいた，日立製作所ビジネスソリューション開発本部の高橋主管技師長をはじめとする幹部の皆様，ならびに先端ミドルウェア開発部の皆様に感謝いたします．また，本論文の内容に関しご議論をいただいた米崎研究室の皆様に感謝いたします．

参考文献

1) Marrero, W., Clarke, E. and Jha, S.: Model Checking for Security Protocols, Research Report, CMU (1997).
2) Burrows, M., Abadi, M. and Needham, R.: A Logic of Authentication, Research Report 39, DEC SRC (1989).
3) Gürgens, S.: SG Logic – A Formal Analysis Thechnique for Authentication Protocols, *Security Protocols 5th International Workshop*, LNCS, Vol.1361, pp.159–176, Springer (1997).
4) 月村賢治，斎藤孝通，Wen, W.：認証プロトコルの解析ツール，日本ソフトウェア科学会第 16 回大会論文集，pp.241–244 (1999).
5) Murayama, Y.: Using BAN Logic for the Proof of a Network Address Registration Protocol, *Trans. IPSJ*, Vol.37, No.5, pp.779–789 (1996).
6) Bird, R., Gopal, I., Herzburg, A., et al.: Systematic Design of Two-Party Authentication Protocols, *Advances in Cryptology CRYPTO'91*, LNCS, Vol.576, pp.44–61, Splinger (1991).
7) Syverson, P.: On Key Distribution Protocols for Repeated Authentication, *SIGOPS Operating Systems Reviw*, Vol.27, No.4, pp.24–30 (1993).
8) Syverson, P.F. and van Oorschot, P.C.: On Unifying Some Cryptographic Protocol Logics, *IEEE Symposium on Research in Security and Privacy*, pp.14–28 (1994).
9) Date, C.: *An Introduction to Database Systems Volume 2*, pp.20–24, Addison-Wesley (1983).
10) ITU: *ITU-T Rec. X.509 | ISO/IEC 9594-8 Information technology – Open Systems Interconnection – The Directory: Authentication Framework* (1997).

付　　録

A.1 推論規則の定義

この付録では，本文中で省略した推論規則の定義を示す．

(1) メッセージの伝達保証

$$\frac{P \models Q\ says\ \overline{\{X\}_Z}\ to\ P \wedge P\ has\ \overline{inv(Z)}}{P \models Q\ says\ \bar{X}\ to\ P}$$

$$\frac{P \models Q\ says\ (\overline{X_1, X_2})\ to\ P}{P \models Q\ says\ \bar{X_1}\ to\ P}$$

(2) 受信

$$\frac{P \lhd \overline{X_1, X_2}}{P \lhd \bar{X_1}}$$

$$\frac{P \lhd \overline{\{X\}_Z} \wedge P\ has\ \overline{inv(Z)}}{P \lhd \bar{X}}$$

(3) 含む

$$\frac{\bar{X}\ in\ \bar{X_1}}{\bar{X}\ in\ (\overline{X_1, X_2})}$$

$$\frac{\bar{X}\ in\ \bar{X_1}}{\bar{X}\ in\ \overline{\{X_1\}_Z}}$$

$$\overline{\bar{X}\ in\ \bar{X}}$$

(4) 名前を含む

$$\frac{P \lhd \bar{X_1} \wedge \bar{X_1}\ in\ \bar{X} \wedge X_1 = P}{P \models \bar{X}\ isto\ P}$$

$$\frac{P \lhd K_{jP}^{w'} \wedge K_{jP}^{w'}\ in\ \bar{X}}{P \models \bar{X}\ isto\ P}$$

$$\frac{P \lhd \overline{\{X_1\}_{K_{jP}}} \wedge \overline{\{X_1\}_{K_{jP}}}\ in\ \bar{X}}{P \models \bar{X}\ isto\ P}$$

$$\frac{P \lhd K_{jPQ}^{w} \wedge K_{jPQ}^{w}\ in\ \bar{X}}{P \models \bar{X}\ isto\ P}$$

$$\frac{P \lhd \overline{\{X_1\}_{K_{jPQ}}} \wedge \overline{\{X_1\}_{K_{jPQ}}}\ in\ \bar{X}}{P \models \bar{X}\ isto\ P}$$

(5) 持っている

$$\frac{P\ has\ \overline{X_1, X_2}}{P\ has\ \bar{X_1}}$$

$$\frac{P\ has\ \overline{\{X\}_Z} \wedge P\ has\ \overline{inv(Z)}}{P\ has\ \bar{X}}$$

$$\frac{P \lhd \bar{X}}{P\ has\ \bar{X}}$$

(平成 11 年 12 月 10 日受付)
(平成 12 年 6 月 1 日採録)

根岸　和義（学生会員）

1973 年東京工業大学工学部電子物理工学科卒業．1975 年同大学院修士課程修了．同年（株）日立製作所入社．同社システム開発研究所において分散データベース，オンラインシステム，マルチプロセッサシステム，電子商取引システム，セキュリティプロトコル検証の研究に従事，特に性能評価，プロトコル検証の研究に興味を持つ．現在，同社ビジネスソリューション開発本部先端ミドルウェア開発部に勤務．また，1997 年 10 月より，東京工業大学情報理工学研究科計算工学専攻にて博士課程在籍中．電子情報通信学会，日本ソフトウェア科学会，ACM，IEEE CS 各会員．

米崎　直樹（正会員）

1972 年東京工業大学工学部電気工学科卒業．1977 年同大学院電子物理工学専攻博士課程修了．工学博士．同大学工学部情報工学科助手，助教授を経て，1991 年東京工業大学工学部情報工学科教授．現在，同大学情報理工学研究科教授．この間 1985 年より 1 年間エディンバラ大学訪問助教授，1991 年より 3 年間北陸先端科学技術大学院大学教授を兼務．パターン情報処理，アルゴリズム等の研究を経て，現在ソフトウェアへの形式手法の適用，特に非標準論理によるソフトウェア検証，推論機構等の研究・教育に従事．AI への論理的アプローチにも興味を持つ．