日本ソフトウェア科学会第 27 回大会 (2010 年度) 講演論文集

暗号文間の関係情報を推論する体系に対する可能世界意味論

萩原 茂樹　小黒 博昭　米崎 直樹

適切なメッセージ集合を想定し，その集合から敵が獲得できる情報を解析することにより，暗号プロトコルの秘密性を検証することができる．著者らはこれまでに，2 つの暗号メッセージの鍵や内容の関係情報すなわち同値性・非同値性を，敵が獲得可能かどうかを解析できる演繹体系と，その意味論を構成した．この意味論では，敵による関係情報の獲得を，敵がその情報を獲得する証拠を提示できることというように，直観主義的に意味定義していた．本論文では，より自然に，この演繹体系を知識の論理と捉え，敵が関係情報を獲得することを，知識として得ることと直接的に定義するような，新たな可能世界意味論を構成する．さらに，これら 2 つの意味論の比較についても議論する．

1　はじめに

情報通信ネットワークが高度に発達し，様々な情報のやりとりが行われている．これら情報の中には，認証に用いるパスワードや，個人のプライバシー情報など，他者に秘密にする必要がある情報も少なくない．これらの情報は暗号通信されるが，暗号化していても，なりすまし攻撃などにより，内容や鍵についての情報が悪意のある敵に知られる可能性がある．秘密にしたい情報の通信を安全に行えるようにするためには，このような可能性の解析手法が必要である．これに対して，これまでに，プロトコルの秘密性や認証，匿名性の検証手法の研究がなされてきた．この中でも，秘密性の解析を行うには，敵が獲得しうる適切なメッセージ集合を想定し，その集合から敵が獲得できる情報を解析する．著者らはこれまでに，[2] により，2 つの暗号メッセージの鍵や内容の関係情報すなわち同値性・非同値性の情報を，敵が獲得可能かどうかを解析できる演繹体系を提案し，[6] により，この体系の部分体系に対して，健全で完全な意味論を構成した．この意味論では，敵による関係情報の獲得を，敵がその情報を獲得する証拠を提示できることというように，直観主義的に意味定義していた．本論文では，より自然に，この論理を知識の論理と捉え，敵が関係情報を獲得することを，知識として得ることと直接的に定義するような，新たな可能世界意味論を構成する．さらに，これら 2 つの意味論を比較し，直観主義的意味論で真となる式は，可能世界意味論でも真となることを示す．これは，[6] の演繹体系が，可能世界意味論に対して健全であることを意味する．

本論文の構成は次のとおりである．まず，2 章で，[6] の論理体系を拡張した論理の構文を述べ，3 章で，その構文に可能世界意味論を与える．そして 4 章で，公理化に関して議論する．次に 5 章で，[6] で与えた意味論と同様の直観主義的意味論を与え，6 章で 2 つの意味論の比較について議論する．7 章で関連研究について述べ，最後に 8 章で成果をまとめる．

Possible worlds semantics for a Deduction System to Derive Relational Information between Ciphertexts

Shigeki Hagihara, Hiroaki Oguro, Naoki Yonezaki, 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 Engineering, Tokyo Institute of Technology.

Hiroaki Oguro, 株式会社 NTT データ 技術開発本部 IT アーキテクチャ&セキュリティ技術センタ, IT Architecture & Security Center, Research and Development Headquarters, NTT DATA Corporation.

2 暗号文間の関係情報の獲得可能性の論理の構文

本章では，2 つの暗号メッセージの鍵や内容の関係情報すなわち同値性・非同値性の情報を，敵が獲得可能かどうかを解析するための論理体系の構文を定義する．

2.1 アルファベット

メッセージを記述するために用いる記号を定義する．定数記号として以下を用いる．

- $\mathcal{K}$：対称鍵記号の集合．
- $\mathcal{I}$：公開アトミックメッセージ記号の集合．
- $\mathcal{N}$：秘密アトミックメッセージ記号の集合．
- $\mathcal{R} = \mathcal{R}_{hon} \cup \mathcal{R}_{adv}$：乱数値を表す記号の集合．
  - $\mathcal{R}_{hon}$：正当な参加者が用いる乱数値を表す記号の集合．
  - $\mathcal{R}_{adv}$：敵が用いる乱数値を表す記号の集合．

さらに，以下の関数記号，述語記号も用いる．

- $content\_of, key\_of$：暗号メッセージの内容や鍵を表す関数記号
- $\equiv, \not\equiv$：等号記号，非等号記号
- $\geqslant$：構成関係を表す記号
- $\wedge, \neg$：古典命題論理の演算子
- $\triangleright$：敵の知識を表す様相演算子

これらの記号を用いて，メッセージと拡張メッセージ，式を定義する．

2.2 メッセージ，拡張メッセージ

メッセージを次のように帰納的に定義する．

1. （対称）鍵記号 $K \in \mathcal{K}$ はメッセージである．
2. 公開アトミックメッセージ記号 $I \in \mathcal{I}$ はメッセージである．
3. 秘密アトミックメッセージ記号 $N \in \mathcal{N}$ はメッセージである．
4. T_1 と T_2 がメッセージであるとき，その連結 (T_1, T_2) はメッセージである．
5. T がメッセージであり，$K \in \mathcal{K}$ が鍵記号，$R \in \mathcal{R}$ が乱数値の記号であるとき，T を K で暗号化したメッセージ $\{T\}_K^R$ はメッセージである．ここで，R は暗号化の際，用いられた乱数値を表す．$\{T\}_K^R$ を暗号メッセージと呼ぶ．

例 1 I と K_2 を連結し，それを K_1 で暗号化し，さらにその結果を K_3 で暗号化してできたメッセージを $\{\{(I, K_2)\}_{K_1}^{R}\}_{K_3}^{R'}$ と表す．ここで，R と R' はそれぞれの暗号化で用いられた乱数値を表す記号である．

暗号メッセージの内容や暗号化に使用された鍵に言及するために，拡張メッセージ E を次のように定義する．

1. メッセージ T は拡張メッセージである．
2. E が拡張メッセージであるとき，$content\_of(E)$, $key\_of(E)$ はそれぞれ拡張メッセージである．

E が暗号メッセージを表している場合，$content\_of(E)$ はその内容を表し，$key\_of(E)$ は E の暗号化に用いられた鍵を表すことを意図し，E が暗号メッセージを表していない場合は，未定義とすることを意図する．

メッセージ用のメタ変数として $T, T', T_1, T_2, \ldots$ を用い，拡張メッセージ用のメタ変数として $E, E', E_1, E_2, \ldots$ を用いる．

2.3 式

メッセージから他のメッセージを新たに構成できることや，2 つの暗号メッセージの内容や暗号化に使用された鍵の等価性や非等価性，さらに，これらの事実を敵が知識として獲得できることに言及するために，式を次のように帰納的に定義する．

1. T_1, T_2 がメッセージであるとき，$T_1 \geqslant T_2$ は式である．
2. E_1, E_2 が拡張メッセージであるとき，$E_1 \equiv E_2$ と $E_1 \not\equiv E_2$ は式である．
3. φ_1, φ_2 が式であるとき，$\varphi_1 \wedge \varphi_2, \neg\varphi_1$ は式である．
4. T がメッセージ，φ が式であるとき，$T \triangleright \varphi$ は式である．

ここで，$T_1 \geqslant T_2$ は T_1 の値から T_2 の値が構成できることを表し，$E_1 \equiv E_2$ は E_1 と E_2 の値が定義され，それらが等しいことを表わす．$E_1 \not\equiv E_2$ は E_1 と E_2 の値が定義され，それらが異なることを表わす†1．

†1 $E_1 \not\equiv E_2$ と $\neg(E_1 \equiv E_2)$ は異なる式である．3 章で定義する意味論においても，これら 2 つの式の意味は

$\varphi_1 \wedge \varphi_2, \neg\varphi_1$, の意味は，古典命題論理における意味と同様である．$T \triangleright \varphi$ はメッセージ T を持っている敵は φ が成り立つことを知識として獲得できることを表す．$T \triangleright \varphi$ の形の式を様相式とよぶ．

例 2 T, T_1, T_2 がメッセージであるとき，$content\_of(T_1) \equiv T_2$ や $key\_of(T_1) \not\equiv key\_of(T_2)$ は式であり，それぞれ「T_1 は暗号メッセージであり，その内容の値が T_2 の値と等しい」こと，「T_1 と T_2 は暗号メッセージであり，そこで用いられている鍵は異なる」ことを表す．$T \triangleright content\_of(T_1) \equiv T_2$ や $T \triangleright key\_of(T_1) \not\equiv key\_of(T_2)$ は様相式であり，「T_1 が暗号メッセージであり，その内容の値が T_2 の値と等しいことを，T を持っている敵は知識として獲得できる」こと，「T_1 と T_2 は暗号メッセージであり，そこで用いられている鍵は異なることを，T を持っている敵は，知識として獲得できる」ことを表す．

3 可能世界意味論

本章では，2 章で定義したメッセージと拡張メッセージ，式に対して，それぞれ意味を与える．特に，敵が知識を持つことを表す様相式に意味を与えるため，可能世界意味論を用いる．可能世界意味論は，知識の論理をはじめとする，様相論理の意味論として広く用いられる．知識の論理の意味論としての可能世界意味論では，様々な状況それぞれを可能世界と捉え，観測者が式が成り立つことを知ることを，観測者が現状況（現可能世界）と違いを識別できないすべての状況（可能世界）おいて，式が成り立つことと意味付けする．本論文においても，様相式に対して同様に意味付けする．

3.1 節，3.2 節，3.3 節で，メッセージ，拡張メッセージ，式に意味を与える．3.4 節では，様相式を中心にいくつかの式に対して，意味解釈を例示する．

3.1 メッセージの意味

メッセージはメッセージ代数で意味付けされる．

異なる．

3.1.1 メッセージ代数

メッセージ代数は組 $\mathcal{A} = \langle A_{key}, A_{pub}, A_{sec}, A_{ct}, A_{pair}, R_{hon}, R_{adv}, pair, enc\rangle$ で定義される．ここで，A_{key} は鍵データの集合，A_{pub} は公開データの集合，A_{sec} は秘密データの集合，A_{ct} は暗号データの集合，A_{pair} は対データの集合である．$A = A_{key} \cup A_{pub} \cup A_{sec} \cup A_{ct} \cup A_{pair}$ をメッセージデータの集合とよぶ．R_{hon} と R_{adv} はそれぞれ，正当な参加者が用いる乱数データの集合と敵が用いる乱数データの集合である．$pair : A^2 \to A_{pair}$ は 2 つのメッセージデータから対データを返す関数である．$enc : A \times A_{key} \times (R_{hon} \cup R_{adv}) \to A_{ct}$ は内容として用いるメッセージデータと鍵データ，乱数データから暗号データを返す暗号化関数である．

また，$A_{key}, A_{pub}, A_{sec}, A_{ct}, A_{pair}$ は交わりがないとする．つまり，メッセージデータがこれらのいずれに属すかは，唯一に定まるとする．

さらに，enc と $pair$ について，次の等式が成り立つこととする．

- $enc(d, k, r) = enc(d', k', r')$
  $\Rightarrow d = d' \wedge k = k' \wedge r = r'$
- $pair(d_1, d_2) = pair(d_3, d_4)$
  $\Rightarrow d_1 = d_3 \wedge d_2 = d_4$

U をメッセージデータの集合とする．このとき，U の閉包 $cl(U)$ は以下を満たすメッセージデータの最小集合 X である．

- $U \subseteq X$
- $A_{pub} \subseteq X$
- $d_1, d_2 \in X \Rightarrow pair(d_1, d_2) \in X$
- $pair(d_1, d_2) \in X \Rightarrow d_1, d_2 \in X$
- $d, k \in X, k \in A_{key}, r \in R_{adv}$
  $\Rightarrow enc(d, k, r) \in X$
- $enc(d, k, r), k \in X \Rightarrow d \in X$

$cl(U)$ は，敵により U から構成されるメッセージデータの集合を表す．

3.1.2 メッセージの意味

$\mathcal{A}$ をメッセージ代数とする．m をアトミックメッセージ記号と乱数値記号に対して，以下のように適切な型のメッセージデータや乱数データを割り当てる付値とする．

- $\mathcal{K}$ の対称鍵記号に対して，A_{key} の鍵データ
- $\mathcal{I}$ の公開アトミックメッセージ記号に対して，A_{pub} の公開データ
- $\mathcal{N}$ の秘密アトミックメッセージ記号に対して，A_{sec} の秘密データ
- $\mathcal{R}_{hon}$ の乱数値記号に対して，R_{hon} の乱数データ
- $\mathcal{R}_{adv}$ の乱数値記号に対して，R_{adv} の乱数データ

ここで，m は異なる記号には異なるデータを割り当てるものとする[†2]．これを用いて，メッセージにメッセージデータを割り当てる付値関数 $[\![\cdot]\!]_{\mathcal{A},m}$ を次のように定義する．

- $[\![K]\!]_{\mathcal{A},m} = m(K)$
- $[\![I]\!]_{\mathcal{A},m} = m(I)$
- $[\![N]\!]_{\mathcal{A},m} = m(N)$
- $[\![(T_1, T_2)]\!]_{\mathcal{A},m} = pair([\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m})$
- $[\![\{T\}_K^R]\!]_{\mathcal{A},m} = enc([\![T]\!]_{\mathcal{A},m}, [\![K]\!]_{\mathcal{A},m}, m(R))$

3.2 拡張メッセージの意味

本節では，拡張メッセージに意味を与える．拡張メッセージでは，暗号メッセージの内容や暗号化に使用された鍵に言及する．敵が暗号メッセージを持っていても，鍵がないとそれがどのような暗号メッセージなのか，つまり，内容や鍵が何かがわからない．それを表現するために，3.2.1 節で暗号データから敵がそれと違いを識別できない暗号データへの置換（再解釈と呼ぶ）を定義する．メッセージの付値に対して，それを再解釈した結果は，敵がそれと違いを識別できない付値となる．様々な再解釈があることが，敵が現付値と違いを識別できない付値が様々あることに対応し，再解釈した結果それぞれが可能世界を構成する．再解釈を用いて，可能世界を表す手法は，[4] により，セキュリティプロトコルの匿名性の検証に用いる知識の論理の意味論で取り入れられたものである．本論文では，対象とする関係情報の知識の論理で用いることできるように，この手法を変更して導入する．そして，定義した再解釈を用いて，3.2.2 節で拡張メッセージに意味を与える．

3.2.1 メッセージデータの再解釈

$U \subseteq A$ を敵が持つメッセージデータの集合とする．このとき，A 上の置換（A から A への全単射）π が以下の条件 1〜6 をみたすとき，U のもとでの準再解釈という．

1. $d \in A_{key} \cup A_{pub} \cup A_{sec} \Rightarrow \pi(d) = d$
2. $\pi(pair(d_1, d_2)) = pair(\pi(d_1), \pi(d_2))$
3. π は暗号データを暗号データに置換する．
4. $enc(d, k, r), k \in U \Rightarrow$
   $\pi(enc(d, k, r)) = enc(\pi(d), k, r)$
5. $d, k \in U, k \in A_{key}, r \in R_{adv} \Rightarrow$
   $\pi(enc(d, k, r)) = enc(\pi(d), k, r)$
6. $enc(d, k, r), k' \in U$ かつ $k \neq k' \Rightarrow$
   $\forall d' \forall r' \pi(enc(d, k, r)) \neq enc(d', k', r')$

π が U のもとでの準再解釈であり，かつ，π^{-1} が $\pi(U)$ のもとでの準再解釈であるとき，π を U のもとでの再解釈という．

$\pi(d_1) = d_2$ であるような U のもとでの再解釈 π が存在することは，U を持つ敵が d_1 を与えられたとき，d_2 との違いを識別できないことを表す．

π をデータの集合に対する関数となるように拡張する．つまり，$\pi(X) = \{\pi(d) | d \in X\}$ とする．

U のもとでの再解釈の集合を $R(U)$ とする．

このとき，性質 1 と性質 2 がそれぞれ成り立つ．

性質 1 *1.* $id \in R(U)$ ここで id は恒等置換
2. $\pi \in R(U)$ ならば $\pi^{-1} \in R(\pi(U))$
3. $\pi \in R(U)$ かつ $\pi' \in R(\pi(U))$ ならば，$\pi' \circ \pi \in R(U)$

(*3* の証明の概略) メッセージデータの集合 X に対して，ν が X のもとでの準再解釈であり，ν' が $\nu(X)$ のもとでの準再解釈であるとき，$\nu' \circ \nu$ は X のもとでの準再解釈であるという補題を最初に示す．これを用いて，$\pi' \circ \pi$ が U のもとでの準再解釈であることと，$(\pi' \circ \pi)^{-1} = \pi^{-1} \circ \pi'^{-1}$ が $\pi'(\pi(U))$ のもとでの準再解釈であることをそれぞれ示す． □

性質 2 $\pi \in R(cl(\{d_1\}))$ かつ，$d_2 \in cl(\{d_1\})$ であるとき，$\pi(d_2) \in cl(\{\pi(d_1)\})$ である．

†2 本意味論において，「m は異なる記号には異なるデータを割り当てる」という制約を含めない定義も可能である．この制約を含めなくても，6 章の定理 1 は成り立つ．6 章で，[6] の演繹体系（付録 A に掲載）が，この意味論に対して健全であることを述べるが，[6] の演繹体系が，この m に対する制約を前提としていたため，ここでは，この制約を意味論に含めた．

(証明の概略) $d_2 \in cl(\{d_1\})$ の定義に関する帰納法による. □

3.2.2 拡張メッセージの意味

π をメッセージデータの再解釈とする. このとき, 拡張メッセージにメッセージデータを割り当てる付値関数 $[\![\cdot]\!]^{\pi}_{\mathcal{A},m}$ を次のように定義する.

- $[\![T]\!]^{\pi}_{\mathcal{A},m} = \pi([\![T]\!]_{\mathcal{A},m})$
- $[\![content\_of(E)]\!]^{\pi}_{\mathcal{A},m} =$
$$\begin{cases} d & \text{if } [\![E]\!]^{\pi}_{\mathcal{A},m} = enc(d,k,r) \\ undef & \text{otherwise} \end{cases}$$
- $[\![key\_of(E)]\!]^{\pi}_{\mathcal{A},m} =$
$$\begin{cases} k & \text{if } [\![E]\!]^{\pi}_{\mathcal{A},m} = enc(d,k,r) \\ undef & \text{otherwise} \end{cases}$$

ここで, $undef$ は未定義をあらわす特別なデータであり, $undef \notin A$ とする. $content\_of(E)$ や $key\_of(E)$ の意味を, E に対する付値を π に従って再解釈し, その結果得られるデータが暗号データであるならば, その内容や鍵の値と定義し, もし, 暗号データでないならば, $undef$ と定義している.

3.3 式の意味

$\mathcal{A}$ をメッセージ代数, m をアトミックメッセージ記号にメッセージデータを割り当てる付値, π を再解釈とする. $\mathcal{A}, m, \pi$ で, 式 φ が真であることを $\mathcal{A}, m, \pi \models_p \varphi$ で表し, 以下のように定義する.

- $\mathcal{A}, m, \pi \models_p T_1 \geqslant T_2 \Leftrightarrow$
  $[\![T_2]\!]^{\pi}_{\mathcal{A},m} \in cl(\{[\![T_1]\!]^{\pi}_{\mathcal{A},m}\})$
- $\mathcal{A}, m, \pi \models_p E_1 \equiv E_2 \Leftrightarrow$
  $[\![E_1]\!]^{\pi}_{\mathcal{A},m} = [\![E_2]\!]^{\pi}_{\mathcal{A},m} \wedge [\![E_1]\!]^{\pi}_{\mathcal{A},m} \neq undef$
- $\mathcal{A}, m, \pi \models_p E_1 \not\equiv E_2 \Leftrightarrow$
  $[\![E_1]\!]^{\pi}_{\mathcal{A},m} \neq [\![E_2]\!]^{\pi}_{\mathcal{A},m}$
  $\wedge [\![E_1]\!]^{\pi}_{\mathcal{A},m} \neq undef \wedge [\![E_2]\!]^{\pi}_{\mathcal{A},m} \neq undef$
- $\mathcal{A}, m, \pi \models_p \varphi_1 \wedge \varphi_2 \Leftrightarrow$
  $\mathcal{A}, m, \pi \models_p \varphi_1 \ \wedge \ \mathcal{A}, m, \pi \models_p \varphi_2$
- $\mathcal{A}, m, \pi \models_p \neg\varphi_1 \Leftrightarrow \mathcal{A}, m, \pi \not\models_p \varphi_1$
- $\mathcal{A}, m, \pi \models_p T \triangleright \varphi \Leftrightarrow$
  $\forall \pi' \in R(\pi(cl([\![T]\!]_{\mathcal{A},m})))(\mathcal{A}, m, \pi' \circ \pi \models_p \varphi)$

$T_1 \geqslant T_2$ が成り立つことを, T_1 の値から T_2 の値を構成できることと意味付けしている. $E_1 \equiv E_2$ ($E_1 \not\equiv E_2$) が成り立つことを, E_1 と E_2 の値が定義され, それらが等しい (異なる) ことと意味付けしている. 命題論理の演算子 $\wedge, \neg$ に対しては通常の意味付けである. 様相式については, 知識の論理の通常の意味と同様に意味を与えている. つまり, $T \triangleright \varphi$ が成り立つことを, T の値から敵が構成できるメッセージデータの集合のもとでの任意の再解釈において, φ がその再解釈した結果で成り立つことと意味付けしている. これは, T の値を持つ敵が φ を知ることを, T の値を持つ敵が, メッセージの現付値と違いを識別できない如何なる付値に対しても, φ が成り立つことと意味付けしている.

恒等置換を id とする. 任意の $\mathcal{A}, m$ において, $\mathcal{A}, m, id \models_p \varphi$ であるとき, φ は可能世界意味論で恒真であるといい, $\models_p \varphi$ と記述する.

3.4 式の意味解釈の例

本節では, いくつかの式の意味解釈を述べる.

例 3 $\models_p (\{N\}^R_K, K) \geqslant N$ である.
$cl(\{[\![(\{N\}^R_K, K)]\!]_{\mathcal{A},m}\}) =$
$cl(\{enc([\![N]\!]_{\mathcal{A},m}, [\![K]\!]_{\mathcal{A},m}, m(R)), [\![K]\!]_{\mathcal{A},m}\})$ より,
$[\![N]\!]_{\mathcal{A},m} \in cl(\{enc([\![N]\!]_{\mathcal{A},m}, [\![K]\!]_{\mathcal{A},m}, m(R)), [\![K]\!]_{\mathcal{A},m}\})$ であるためである. これは, 暗号メッセージ $\{N\}^R_K$ と鍵 K があれば, 内容 N を取り出せるという事実を表している.

例 4 $\models_p (\{N\}^R_K, K) \triangleright (\{N\}^R_K, K) \geqslant N$ である.
例 *3* と再解釈の性質 *2* より明らかである. これは, 暗号メッセージ $\{N\}^R_K$ と鍵 K を持つ敵は, それらのメッセージがあれば, 内容 N を取り出せることを, 知識として獲得できることを表す.

例 5 $\models_p content\_of(\{N\}^R_K) \equiv N$ である. なぜなら, $[\![\{N\}^R_K]\!]^{id}_{\mathcal{A},m} = id([\![\{N\}^R_K]\!]_{\mathcal{A},m}) = [\![\{N\}^R_K]\!]_{\mathcal{A},m} = enc([\![N]\!]_{\mathcal{A},m}, [\![K]\!]_{\mathcal{A},m}, m(R))$ が成り立ち,
$[\![content\_of(\{N\}^R_K)]\!]^{id}_{\mathcal{A},m} = [\![N]\!]_{\mathcal{A},m} = [\![N]\!]^{id}_{\mathcal{A},m}$ を満たすためである. これは, $\{N\}^R_K$ は暗号メッセージであり, その内容は N であるという事実を表している.

例 6 $\models_p (\{N\}^R_K, K) \triangleright content\_of(\{N\}^R_K) \equiv N$ である. なぜなら
$\mathcal{A}, m, id \models_p (\{N\}^R_K, K) \triangleright content\_of(\{N\}^R_K) \equiv N$
$\Leftrightarrow \forall \pi \in R(id(cl([\![(\{N\}^R_K, K)]\!]_{\mathcal{A},m})))$
$\mathcal{A}, m, \pi \circ id \models_p content\_of(\{N\}^R_K) \equiv N$

$\Leftrightarrow \forall \pi \in R(cl([\![(\{N\}_K^R, K)]\!]_{\mathcal{A},m}))$
$\mathcal{A}, m, \pi \models_p content\_of(\{N\}_K^R) \equiv N$
$\Leftrightarrow \forall \pi \in R(cl(\{enc([\![N]\!]_{\mathcal{A},m}, [\![K]\!]_{\mathcal{A},m}, m(R)), [\![K]\!]_{\mathcal{A},m}\}))$
$[\![content\_of(\{N\}_K^R)]\!]^{\pi}_{\mathcal{A},m} = [\![N]\!]^{\pi}_{\mathcal{A},m}$
ここで，$enc([\![N]\!]_{\mathcal{A},m}, [\![K]\!]_{\mathcal{A},m}, m(R)), [\![K]\!]_{\mathcal{A},m} \in cl(\{enc([\![N]\!]_{\mathcal{A},m}, [\![K]\!]_{\mathcal{A},m}, m(R)), [\![K]\!]_{\mathcal{A},m}\})$ であるため，$\pi \in R(cl(\{enc([\![N]\!]_{\mathcal{A},m}, [\![K]\!]_{\mathcal{A},m}, m(R)), [\![K]\!]_{\mathcal{A},m}\}))$ であるとき，以下を満たす．
$[\![\{N\}_K^R]\!]^{\pi}_{\mathcal{A},m} = \pi([\![\{N\}_K^R]\!]_{\mathcal{A},m})$
$= \pi(enc([\![N]\!]_{\mathcal{A},m}, [\![K]\!]_{\mathcal{A},m}, m(R)))$
$= enc(\pi([\![N]\!]_{\mathcal{A},m}), [\![K]\!]_{\mathcal{A},m}, m(R)))$ よって，
$[\![content\_of(\{N\}_K^R)]\!]^{\pi}_{\mathcal{A},m} = \pi([\![N]\!]_{\mathcal{A},m}) = [\![N]\!]^{\pi}_{\mathcal{A},m}$
よって，題意を満たす．
これは，暗号メッセージ $\{N\}_K^R$ と復号する鍵 K を敵が持っていれば，その内容が N であることを敵が知ることを意味している．

例 7 $\models_p \{N\}_K^R \triangleright content\_of(\{N\}_K^R) \equiv N$ ではない．なぜなら，
$\mathcal{A}, m, id \models_p \{N\}_K^R \triangleright content\_of(\{N\}_K^R) \equiv N$
$\Leftrightarrow \forall \pi \in R(cl(enc([\![N]\!]_{\mathcal{A},m}, [\![K]\!]_{\mathcal{A},m}, m(R))))$
$[\![content\_of(\{N\}_K^R)]\!]^{\pi}_{\mathcal{A},m} = [\![N]\!]^{\pi}_{\mathcal{A},m}$
ここで，$[\![K]\!]_{\mathcal{A},m} \notin cl(enc([\![N]\!]_{\mathcal{A},m}, [\![K]\!]_{\mathcal{A},m}, m(R)))$ より，次の π は $cl(enc([\![N]\!]_{\mathcal{A},m}, [\![K]\!]_{\mathcal{A},m}, m(R)))$ のもとでの再解釈である．ここで，$[\![N]\!]_{\mathcal{A},m} \neq n'$ とする．

$$\pi = \left(\begin{array}{c} enc([\![N]\!]_{\mathcal{A},m}, [\![K]\!]_{\mathcal{A},m}, m(R)) \mapsto enc(n', k', r') \\ enc(n', k', r') \mapsto enc([\![N]\!]_{\mathcal{A},m}, [\![K]\!]_{\mathcal{A},m}, m(R)) \\ [\![N]\!]_{\mathcal{A},m} \mapsto [\![N]\!]_{\mathcal{A},m} \\ [\![K]\!]_{\mathcal{A},m} \mapsto [\![K]\!]_{\mathcal{A},m} \\ n' \mapsto n' \\ k' \mapsto k' \end{array} \right)$$

このとき，以下を満たす．
$[\![\{N\}_K^R]\!]^{\pi}_{\mathcal{A},m} = \pi([\![\{N\}_K^R]\!]_{\mathcal{A},m})$
$= \pi(enc([\![N]\!]_{\mathcal{A},m}, [\![K]\!]_{\mathcal{A},m}, m(R))) = enc(n', k', r')$
よって，$[\![content\_of(\{N\}_K^R)]\!]^{\pi}_{\mathcal{A},m} = n' \neq [\![N]\!]_{\mathcal{A},m}$
$= \pi([\![N]\!]_{\mathcal{A},m}) = [\![N]\!]^{\pi}_{\mathcal{A},m}$
よって，題意を満たす．
これは，暗号メッセージ $\{N\}_K^R$ しか敵が持っていないならば，その内容が N であることは敵には知られないことを意味している．

例 8 $R \in \mathcal{R}_{adv}$ であるとき，$\models_p (N, K) \triangleright content\_of(\{N\}_K^R) \equiv N$ である．例 6 と同様の理由による．これは，暗号メッセージ $\{N\}_K^R$ は敵自身が作成するメッセージなので，その内容が N であることを敵が知っていることを意味している．

4 公理系構築へ向けての議論

恒真式を導出する公理系を構成するために，どのような式が公理となるだろうか．次の式は恒真であり，公理になりうる．

- 古典命題論理の公理
- 等号 $\equiv$，非等号 $\not\equiv$ に関する性質．例えば
  - $E \equiv E$
  - $E_1 \equiv E_2 \rightarrow E_2 \equiv E_1$
  - $E_1 \equiv E_2 \wedge E_2 \equiv E_3 \rightarrow E_1 \equiv E_3$
  - $\cdots$
- $content\_of, key\_of$ について
  - $content\_of(\{T\}_K^R) \equiv T$
  - $key\_of(\{T\}_K^R) \equiv K$
- 知識の論理の通常の公理 (再解釈の性質 1 より)
  - $T \triangleright (\varphi \rightarrow \psi) \rightarrow (T \triangleright \varphi \rightarrow T \triangleright \psi)$
  - $T \triangleright \varphi \rightarrow \varphi$
  - $T \triangleright \varphi \rightarrow T \triangleright T \triangleright \varphi$
  - $\neg T \triangleright \neg\varphi \rightarrow T \triangleright \neg T \triangleright \neg\varphi$
- 知識の単調性
  - $T_1 \geqslant T_2 \rightarrow (T_2 \triangleright \varphi \rightarrow T_1 \triangleright \varphi)$

一方，例 5 と例 6，例 7 より，$\models_p \varphi$ であっても，$\models_p T \triangleright \varphi$ であるとは限らない．つまり，この論理では，多くの様相論理で成り立つ一般化規則 $\vdash \varphi \Rightarrow \vdash T \triangleright \varphi$ は，そのままでは公理にはなりえない．その原因は，恒真の定義方法にある．つまり，$\models_p \varphi$ を，任意の $\mathcal{A}, m$ において $\mathcal{A}, m, id \models_p \varphi$ であることと定義したため，一般化規則が成り立たない．任意の $\mathcal{A}, m, \pi$ において $\mathcal{A}, m, \pi \models_p \varphi$ であることと定義すれば，一般化規則は成り立つ．ところが，得られる論理は，我々の意図しないものとなってしまう．

一方，T と φ の形によっては，一般化規則になりうる規則がある．例えば，次のような規則である．

- $\vdash T_1 \geqslant T_2 \Rightarrow \vdash T_1 \triangleright T_1 \geqslant T_2$ (再解釈の性質 2 より)

完全な公理系を構成するためには，$\models_p \varphi \Rightarrow \models_p T \triangleright \varphi$ が成り立つような，T と φ の特徴を見つける必要がある．

5 証拠構成可能性に基づく直観主義的意味論

本章では，[6] で提案した，証拠構成可能性に基づいて定義した直観主義的な意味論を述べる．3 章では，可能世界意味論を用いて，敵が関係情報を獲得することを，敵が関係情報を知ることと直接的に意味定義していたが，[6] の意味論では，可能世界意味論を用いず，敵が関係情報を獲得することを，敵がその情報を獲得できる証拠を構成できることと直観主義的に定義している．つまり，証拠が閉包の中に含まれることと定義する．[6] では，確率的多項式時間チューリング機械を用いた計算論による意味を提案しているが，本論文では，メッセージ代数を用いた記号的な意味論として再定義する．

2 章で述べた構文のサブセットに対して，この直観主義的意味論を定義する．まず，5.1 節で，この構文制限を述べる．次に，5.2 節で，証拠構成可能性に基づく直観主義的意味論を定義する．

5.1 構文の制限

本意味論では，次の形の式のみを対象とする．

- $T_1 \geqslant T_2$
- $T \triangleright E_1 \equiv E_2, T \triangleright E_1 \not\equiv E_2$
  ここで，E_1, E_2 は $content\_of(T')$,$key\_of(T')$,T' のいずれかの形をしている拡張メッセージとする．

5.2 直観主義的意味論

メッセージの意味は，3.1 節で述べた定義をそのまま用いる．

$\mathcal{A}$ をメッセージ代数，m をアトミックメッセージ記号にメッセージデータを割り当てる付値とする．$\mathcal{A}, m$ で，式 φ が真であることを $\mathcal{A}, m \models_c \varphi$ で表し，以下のように定義する．

式 $T_1 \geqslant T_2$ の意味は 3.3 節で述べた定義と同様である．

- $\mathcal{A}, m \models_c T_1 \geqslant T_2 \Leftrightarrow [\![T_2]\!]_{\mathcal{A},m} \in cl(\{[\![T_1]\!]_{\mathcal{A},m}\})$

式 $T \triangleright E_1 \equiv E_2$ と $T \triangleright E_1 \not\equiv E_2$ の意味は，拡張メッセージ E_1, E_2 の形により，次の 12 通りで定義する．

1. $T \triangleright T_1 \equiv T_2$
   T が与えられたとき，T_1 と T_2 の値が同じである証拠を，敵が構成できるとは，T の値から T_1 と T_2 の値を構成でき，それらが等しいことである．
   $\mathcal{A}, m \models_c T \triangleright T_1 \equiv T_2 \Leftrightarrow$
   $[\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m} \in cl([\![T]\!]_{\mathcal{A},m})$
   $\wedge [\![T_1]\!]_{\mathcal{A},m} = [\![T_2]\!]_{\mathcal{A},m}$
2. $T \triangleright T_1 \not\equiv T_2$
   T が与えられたとき，T_1 と T_2 の値が異なる証拠を，敵が構成できるとは，T の値から T_1 と T_2 の値を構成でき，それらが異なることである．
   $\mathcal{A}, m \models_c T \triangleright T_1 \not\equiv T_2 \Leftrightarrow$
   $[\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m} \in cl([\![T]\!]_{\mathcal{A},m})$
   $\wedge [\![T_1]\!]_{\mathcal{A},m} \neq [\![T_2]\!]_{\mathcal{A},m}$
3. $T \triangleright content\_of(T_1) \equiv T_2$
   T が与えられたとき，T_1 の内容の値が T_2 の値と等しい証拠を，敵が構成できるとは，T の値から T_1 と T_2 の値を構成でき，T_1 の値が暗号データであり，T_1 の値の復号に成功する鍵 k も構成し，復号の結果得られる T_1 の値の内容が T_2 の値と等しいことである．
   $\mathcal{A}, m \models_c T \triangleright content\_of(T_1) \equiv T_2 \Leftrightarrow$
   $\exists k([\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m}, k \in cl([\![T]\!]_{\mathcal{A},m}) \wedge$
   $[\![T_1]\!]_{\mathcal{A},m} \in A_{ct} \wedge k \in A_{key} \wedge$
   $dec([\![T_1]\!]_{\mathcal{A},m}, k) = [\![T_2]\!]_{\mathcal{A},m})$
   ここで，dec は以下を満たす関数（復号関数）とし，$\perp$ は復号失敗を表す特別なデータとする．
   $$dec(d,k) = \begin{cases} d_1 & \text{ある } r \text{ で } d = enc(d_1, k, r) \\ \perp & \text{otherwise} \end{cases}$$
4. $T \triangleright content\_of(T_1) \not\equiv T_2$
   T が与えられたとき，T_1 の内容の値が T_2 の値と異なる証拠を，敵が構成できるとは，T の値から T_1 と T_2 の値を構成し，T_1 の値が暗号データであり，T_1 の値の復号に成功する鍵 k も構成し，復号の結果得られる T_1 の値の内容が T_2 の値と異なることである．
   $\mathcal{A}, m \models_c T \triangleright content\_of(T_1) \not\equiv T_2 \Leftrightarrow$
   $\exists k([\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m}, k \in cl([\![T]\!]_{\mathcal{A},m}) \wedge$
   $[\![T_1]\!]_{\mathcal{A},m} \in A_{ct} \wedge k \in A_{key} \wedge$
   $dec([\![T_1]\!]_{\mathcal{A},m}, k) \neq \perp \wedge dec(e_1, k) \neq [\![T_2]\!]_{\mathcal{A},m})$
5. $T \triangleright content\_of(T_1) \equiv content\_of(T_2)$
   T が与えられたとき，T_1 の内容の値が T_2 の内

容の値と等しい証拠を，敵が構成できるとは，T の値から T_1 と T_2 の値を構成し，それらが暗号データであり，それらが同じ値であるか，T_1 の値と T_2 の値の復号にそれぞれ成功する鍵 k, k' を構成し，復号して得られる内容が等しいことである．

$\mathcal{A}, m \models_c T \triangleright content\_of(T_1) \equiv content\_of(T_2) \Leftrightarrow$
$\exists k, k'([\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m}, k, k' \in cl([\![T]\!]_{\mathcal{A},m}) \wedge$
$[\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m} \in A_{ct} \wedge$
$([\![T_1]\!]_{\mathcal{A},m} = [\![T_2]\!]_{\mathcal{A},m} \vee$
$(k, k' \in A_{key} \wedge dec([\![T_1]\!]_{\mathcal{A},m}, k) \neq \bot \wedge$
$dec([\![T_1]\!]_{\mathcal{A},m}, k) = dec([\![T_2]\!]_{\mathcal{A},m}, k'))))$

6. $T \triangleright content\_of(T_1) \not\equiv content\_of(T_2)$

T が与えられたとき，T_1 の内容の値が T_2 の内容の値と異なる証拠を，敵が構成できるとは，T の値から T_1 と T_2 の値を構成し，それらが暗号データであり，T_1 の値と T_2 の値の復号にそれぞれ成功する鍵 k, k' を構成し，復号して得られる内容が異なることである．

$\mathcal{A}, m \models_c T \triangleright content\_of(T_1) \not\equiv content\_of(T_2) \Leftrightarrow$
$\exists k, k'([\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m}, k, k' \in cl([\![T]\!]_{\mathcal{A},m}) \wedge$
$[\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m} \in A_{ct} \wedge k, k' \in A_{key} \wedge$
$dec([\![T_1]\!]_{\mathcal{A},m}, k) \neq \bot \wedge \quad dec([\![T_2]\!]_{\mathcal{A},m}, k') \neq \bot$
$\wedge dec([\![T_1]\!]_{\mathcal{A},m}, k) \neq dec([\![T_2]\!]_{\mathcal{A},m}, k'))$

7. $T \triangleright key\_of(T_1) \equiv T_2$

T が与えられたとき，T_1 の鍵の値が T_2 の値と等しい証拠を，敵が構成できるとは，T の値から T_1 と T_2 の値を構成し，T_1 の値が暗号データであり，T_1 の値の T_2 の値による復号が成功することである．

$\mathcal{A}, m \models_c T \triangleright key\_of(T_1) \equiv T_2 \Leftrightarrow$
$[\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m} \in cl([\![T]\!]_{\mathcal{A},m}) \wedge$
$[\![T_1]\!]_{\mathcal{A},m} \in A_{ct} \wedge [\![T_2]\!]_{\mathcal{A},m} \in A_{key} \wedge$
$dec([\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m}) \neq \bot$

8. $T \triangleright key\_of(T_1) \not\equiv T_2$

T が与えられたとき，T_1 の鍵の値が T_2 の値と異なる証拠を，敵が構成できるとは，T の値から T_1 と T_2 の値を構成し，T の値が暗号データであり，T_2 の値が鍵ではない又は T_1 の値の T_2 の値による復号が失敗することである．

$\mathcal{A}, m \models_c T \triangleright key\_of(T_1) \not\equiv T_2 \Leftrightarrow$
$[\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m} \in cl([\![T]\!]_{\mathcal{A},m}) \wedge$
$[\![T_1]\!]_{\mathcal{A},m} \in A_{ct} \wedge$
$([\![T_2]\!]_{\mathcal{A},m} \notin A_{key} \vee dec([\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m}) = \bot)$

9. $T \triangleright key\_of(T_1) \equiv key\_of(T_2)$

T が与えられたとき，T_1 の鍵の値が T_2 の鍵の値と等しい証拠を，敵が構成できるとは，T の値から T_1 と T_2 の値を構成し，それらが暗号データであり，それらが同じ値であるか，T_1 の値と T_2 の値を同時に復号できる鍵 k を構成することである．

$\mathcal{A}, m \models_c T \triangleright key\_of(T_1) \equiv key\_of(T_2) \Leftrightarrow$
$\exists k([\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m}, k \in cl([\![T]\!]_{\mathcal{A},m}) \wedge$
$[\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m} \in A_{ct} \wedge$
$([\![T_1]\!]_{\mathcal{A},m} = [\![T_2]\!]_{\mathcal{A},m} \vee$
$(k \in A_{key} \wedge dec([\![T_1]\!]_{\mathcal{A},m}, k) \neq \bot \wedge$
$dec([\![T_2]\!]_{\mathcal{A},m}, k) \neq \bot)))$

10. $T \triangleright key\_of(T_1) \not\equiv key\_of(T_2)$

T が与えられたとき，T_1 の鍵の値が T_2 の鍵の値と異なる証拠を，敵が構成できるとは，T の値から T_1 と T_2 の値を構成し，それらが暗号データであり，T_1 の値と T_2 の値のどちらか片方だけを復号できる鍵 k を構成することである．

$\mathcal{A}, m \models_c T \triangleright key\_of(T_1) \not\equiv key\_of(T_2) \Leftrightarrow$
$\exists k([\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m}, k \in cl([\![T]\!]_{\mathcal{A},m}) \wedge$
$[\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m} \in A_{ct} \wedge k \in A_{key} \wedge$
$((dec([\![T_1]\!]_{\mathcal{A},m}, k) \neq \bot \wedge dec([\![T_2]\!]_{\mathcal{A},m}, k) = \bot) \vee$
$(dec([\![T_1]\!]_{\mathcal{A},m}, k) = \bot \wedge dec([\![T_2]\!]_{\mathcal{A},m}, k) \neq \bot)))$

11. $T \triangleright content\_of(T_1) \equiv key\_of(T_2)$

T が与えられたとき，T_1 の内容の値が T_2 の鍵の値と等しい証拠を，敵が構成できるとは，T の値から T_1 と T_2 の値を構成し，それらが暗号データであり，T_1 の値の復号に成功する鍵 k も構成し，その内容を鍵とする T_2 の値の復号に成功することである．

$\mathcal{A}, m \models_c T \triangleright content\_of(T_1) \equiv key\_of(T_2) \Leftrightarrow$
$\exists k([\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m}, k \in cl([\![T]\!]_{\mathcal{A},m}) \wedge$
$[\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m} \in A_{ct} \wedge$
$k, dec([\![T_1]\!]_{\mathcal{A},m}, k) \in A_{key} \wedge$

$dec([\![T_2]\!]_{\mathcal{A},m}, dec([\![T_1]\!]_{\mathcal{A},m}, k)) \neq \bot$)

12. $T \triangleright content\_of(T_1) \not\equiv key\_of(T_2)$

T が与えられたとき，T_1 の内容の値が T_2 の鍵の値と異なる証拠を，敵が構成できるとは，T の値から T_1 と T_2 の値を構成し，それらが暗号データであり，T_1 の値の復号に成功する鍵 k も構成し，その内容が鍵でない又は鍵として T_2 の値の復号に失敗することである．

$\mathcal{A}, m \models_c T \triangleright content\_of(T_1) \not\equiv key\_of(T_2) \Leftrightarrow$
$\exists k([\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m}, k \in cl([\![T]\!]_{\mathcal{A},m}) \wedge$
$[\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m} \in A_{ct} \wedge k \in A_{key} \wedge$
$dec([\![T_1]\!]_{\mathcal{A},m}, k) \neq \bot \wedge$
$(dec([\![T_1]\!]_{\mathcal{A},m}, k) \notin A_{key} \vee$
$dec([\![T_2]\!]_{\mathcal{A},m}, dec([\![T_1]\!]_{\mathcal{A},m}, k)) = \bot))$

任意の $\mathcal{A}, m$ において，$\mathcal{A}, m \models_c \varphi$ であるとき，直観主義的意味論で φ は恒真であるといい，$\models_c \varphi$ と記述する．

[6] では，敵による関係情報の獲得可能性を演繹する体系を導入している．この体系は，5 章で述べた構文制限された式を対象としており，これを付録 A で紹介する．この体系で式 φ が演繹可能であるとき，$\vdash_{JD} \varphi$ と記述する．この体系は，直観主義的意味論に対して健全で完全である．つまり，以下の命題を満たす．

命題 1 *φ を 5.1 節で述べた構文制限を満たす式とする．このとき，$\models_c \varphi$ iff $\vdash_{JD} \varphi$*

6 2 つの意味論の関係

3 章で定義した可能世界意味論と，5 章で定義した直観主義的意味論について，次の関係が成り立つ．

定理 1 *φ を 5.1 節で述べた構文制限を満たす式とする．$\mathcal{A}$ をメッセージ代数，m をアトミックメッセージ記号にメッセージデータを割り当てる付値とする．このとき，$\mathcal{A}, m \models_c \varphi$ ならば，$\mathcal{A}, m, id \models_p \varphi$ である．*

(証明) この定理は，φ の形の場合分けにより証明できる．φ が $T \triangleright content\_of(T_1) \equiv T_2$ の形の場合の証明は次のとおりである．

$\mathcal{A}, m \models_c T \triangleright content\_of(T_1) \equiv T_2$ であると仮定する．つまり，$[\![T_1]\!]_{\mathcal{A},m}, [\![T_2]\!]_{\mathcal{A},m}, k \in cl([\![T]\!]_{\mathcal{A},m}) \wedge$ $[\![T_1]\!]_{\mathcal{A},m} \in A_{ct} \wedge k \in A_{key} \wedge dec([\![T_1]\!]_{\mathcal{A},m}, k) = [\![T_2]\!]_{\mathcal{A},m}$ であると仮定する．このとき，$[\![T_1]\!]_{\mathcal{A},m} \in A_{ct} \wedge k \in A_{key} \wedge dec([\![T_1]\!]_{\mathcal{A},m}, k) = [\![T_2]\!]_{\mathcal{A},m}$ より，ある r が存在して，$[\![T_1]\!]_{\mathcal{A},m} = enc([\![T_2]\!]_{\mathcal{A},m}, k, r)$ である．よって，π を $\pi \in R(cl([\![T]\!]_{\mathcal{A},m}))$ を満たす再解釈とすると，以下が成り立つ．

$[\![T_1]\!]^{\pi}_{\mathcal{A},m} = \pi([\![T_1]\!]_{\mathcal{A},m}) = \pi(enc([\![T_2]\!]_{\mathcal{A},m}, k, r))$

ここで，$[\![T_1]\!]_{\mathcal{A},m}, k \in cl([\![T]\!]_{\mathcal{A},m})$ と準再解釈の条件 4 より，$\pi(enc([\![T_2]\!]_{\mathcal{A},m}, k, r)) = enc(\pi([\![T_2]\!]_{\mathcal{A},m}), k, r)$ が成り立つ．よって，以下が成り立つ

$[\![content\_of(T_1)]\!]^{\pi}_{\mathcal{A},m} = \pi([\![T_2]\!]_{\mathcal{A},m}) = [\![T_2]\!]^{\pi}_{\mathcal{A},m}$

よって，$\mathcal{A}, m, \pi \models_p content\_of(T_1) \equiv T_2$ が成り立ち，$\mathcal{A}, m, id \models_p T \triangleright content\_of(T_1) \equiv T_2$ が成り立つ．

φ が他の形をした式の場合も同様に証明することができる． □

一方，定理 1 の逆の性質は成り立たない．例えば，$N \triangleright content\_of(\{N\}^R_K) \equiv content\_of(\{N\}^R_K)$ は，可能世界意味論で恒真であるが，直観主義的意味論では恒真ではない．

命題 1 が成り立つので，定理 1 は，付録 A で述べた [6] の体系で演繹される式は，可能世界意味論で恒真となることを意味する．つまり，[6] の演繹体系が本論文で提案した可能世界意味論に対して健全であることを意味する．

系 1 *φ を 5.1 節で述べた構文制限を満たす式とする．このとき，$\vdash_{JD} \varphi$ ならば，$\models_p \varphi$ である．*

7 関連研究

知識の論理を用いたプロトコルの安全性の検証手法の研究には様々な研究がある．認証プロトコルにおいて，正しく認証できることを検証する手法の研究として，BAN 論理 [3] がある．BAN 論理は知識の論理とみなすことができ，[1] で可能世界意味論を用いて意味を与えられた．認証が正しく行えることを BAN 論理で記述し，プロトコルの定義より得られる公理からそれを導出することで検証する．BAN 論理を発展させた論理も様々提案されている．

知識の論理を用いたプロトコルの匿名性の検証手法の研究としては，[5] や [4] 等がある．匿名性を満た

すことを，知識の論理で記述し，それがプロトコルにおける参加者の振る舞いモデルで成り立つことを示すことで検証する．

認証や匿名性は，メッセージの送受信を基本に定義されるため，これらの論理では，メッセージの送受信を表す命題を用いる．一方，本論文で提案した論理は，プロトコルの秘密性，特に暗号文間の関係情報の秘密性の検証に用いることを意図した論理であるため，同値関係，非同値関係を表す命題を用いる．この点で，これらの論理とは異なる．

8 まとめ

本論文では，暗号メッセージの鍵や内容の関係情報すなわち同値性・非同値性の情報を，敵が獲得可能かどうかを解析するための論理に，新たな可能世界意味論を構成した．ここでは，敵が獲得できる同値性・非同値性の情報を，敵の知識とみなすことにより，知識の論理として意味論を構成した．この意味論は，敵の獲得情報を知識とみなしているという点で，[6] で構成していた直観主義的な意味論と比較して，より自然に定義された意味論となっている．この可能世界意味論と直観主義的意味論との比較を行い，直観主義的な意味論で真となる式は，同じモデルで可能世界意味論でも真となることを示した．これは，この可能世界意味論が，[6] で提案された，構文制限された式に対する演繹規則のための，健全な意味論となっていることを意味する．

この論理は，セキュリティプロトコルにおいて，暗号文間の関係情報の秘密性を解析することを意図した論理である．例えば，過去に送信された暗号メッセージで利用された鍵と，現在送信されている暗号メッセージ鍵が同値あるいは非同値という情報が，敵に知られるかどうかを解析することを意図している．この論理の公理系が構成できると，公理系からの演繹による解析が可能となる．この可能世界意味論に対して，健全な（出来れば完全な）公理系を構築することが今後の課題である．

参 考 文 献

[1] Martín Abadi and Mark R. Tuttle. A semantics of a logic of authentication. In *Proceedings of the Tenth Annual ACM Symbosium of Principles of Distributed Computing*, pp. 201–216, 1991.

[2] Ashraf Bhery, Shigeki Hagihara, and Naoki Yonezaki. A formal system for analysis of cryptographic encryption and their security properties. In *International Symposium on Software Security 2003, Software Security - Theories and Systems*, Vol. 3233 of *Lecture Notes in Computer Science*, pp. 87–112, 2004.

[3] Michael Burrows, Martín Abadi, and Roger Needham. A logic of authentication. *ACM Transactions on Computer Systems*, Vol. 8, No. 1, pp. 18–36, 1990.

[4] Flavio D. Garcia, Ichiro Hasuo, Wolter Pieters, and Peter van Rossum. Provable anonymity. In *FMSE '05: Proceedings of the 2005 ACM workshop on Formal methods in security engineering*, pp. 63–72, New York, NY, USA, 2005. ACM.

[5] J.Y. Halpern and K.R. O'Neill. Anonymity and information hiding in multiagent systems. In *Computer Security Foundations Workshop, 2003. Proceedings. 16th IEEE*, pp. 75 – 88, 30 2003.

[6] 萩原茂樹, 小黒博昭, 米崎直樹. 暗号文から得られる部分情報に関する推論体系とその計算論に基づく意味. 日本ソフトウェア科学会第 24 回大会講演論文集, 2007.

A 敵による関係情報の獲得可能性を演繹する体系

[6] で導入された，敵による関係情報の獲得可能性を演繹する体系を紹介する．この体系は，5 章で述べた構文制限された式を対象としている．

$T_1 \geqslant T_2$ の形の式を演繹する規則は次のとおりである．

$$\frac{}{\overline{T \geqslant T} \quad \overline{T \geqslant I}} \ (\text{ここで，} I \in \mathcal{I})$$

$$\frac{T \triangleright T_1 \quad T \geqslant T_1}{T \triangleright (T_1, T_2)} \qquad \frac{T \geqslant (T_1, T_2)}{T \geqslant T_1} \qquad \frac{T \geqslant (T_1, T_2)}{T \geqslant T_2}$$

$$\frac{T \geqslant \{T_1\}_K^R \quad T \geqslant K}{T \geqslant T_1}$$

$$\frac{T \geqslant T_1 \quad T \geqslant K}{T \geqslant \{T_1\}_K^R} \ (\text{ここで，} R \in \mathcal{R}_{adv})$$

$T \triangleright E_1 \equiv E_2$ や $T \triangleright E_1 \not\equiv E_2$ の形の式を演繹する規則は次のとおりである．

$$\frac{T \geqslant T_1}{T \triangleright T_1 \equiv T_1}$$

$$\frac{T \geqslant T_1 \quad T \geqslant T_2}{T \triangleright T_1 \not\equiv T_2} \quad (\text{ここで，} T_1 \text{ と } T_2 \text{ は構文的}$$

に異なるメッセージ)

$$\frac{T \triangleright \{T_1\}_K^R \equiv \{T_2\}_{K'}^{R'}}{T \triangleright f(\{T_1\}_K^R) \equiv f(\{T_2\}_{K'}^{R'})}$$

(f は $content\_of, key\_of$ のいずれか)

$$\frac{T \geqslant \{T_1\}_K^R \quad T \geqslant K}{T \triangleright content\_of(\{T_1\}_K^R) \equiv T_1}$$

$$\frac{T \geqslant \{T_1\}_K^R \quad T \geqslant K}{T \triangleright key\_of(\{T_1\}_K^R) \equiv K}$$

$$\frac{T \geqslant \{T_1\}_K^R \quad T \geqslant T_2}{T \triangleright key\_of(\{T_1\}_K^R) \not\equiv T_2}$$

(T_2 は構文的に K と異なるメッセージ)

$$\frac{T \triangleright E_1 \equiv E}{T \triangleright E \equiv E_1} \qquad \frac{T \triangleright E_1 \not\equiv E}{T \triangleright E \not\equiv E_1}$$

$$\frac{T \triangleright E \equiv E_2 \quad T \triangleright E_2 \equiv E_1}{T \triangleright E \equiv E_1}$$

$$\frac{T \triangleright E \equiv E_2 \quad T \triangleright E_2 \not\equiv E_1}{T \triangleright E \not\equiv E_1}$$

これらの規則により，式 φ が導出されるとき，$\vdash_{JD} \varphi$ と記述する．