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

2006－IS－95 (1)
2006／3／16

個人情報保護と情報公開を考慮した介護・医療分野向け情報フロー監視システムの提案

森住哲也† 木下宏揚††
寺谷 葉津希‡ 永瀬 宏‡

† 東洋ネットワークシステムズ株式会社 〒212-8452 川崎市幸区塚越 3-484
†† 神奈川大学工学部・ハイテクリサーチセンター 〒221-8686 横浜市神奈川区六角橋 3-27-1
‡ 金沢工業大学情報工学科 〒921-8501 石川県石川郡野々市町扇が丘 7-1

E-mail: †moriz@olive.ocn.ne.jp ††kino@cs.ee.kanagawa-u.ac.jp ‡ hnagase@neptune.kanazawa-it.ac.jp

あらまし 介護医療の情報処理をシステム化する時，個人情報の漏えいや競合するコミュニティ間の情報漏えいが問題になる．対策としてアクセス制御技術を使う場合，アクセス行列では許可されていないはずの情報の内容が伝播する Covert Channel を分析制御する事が重要である．なぜなら，介護・医療と言う社会システムは，機能分化する社会システムの競合的，連携的な環境の中で個人情報が使われるからであり，かつまた個人情報は決して情報漏えいや改ざんされてはならないからである．本稿ではこの問題解決のために Community Based Access Control Model を適用する事を試み，問題解決の1つの提案とする．

キーワード 介護医療，セキュリティモデル,アクセス制御,Covert Channel, Web アプリケーションシステム,社会システム

Proposal of information flow monitoring system for nursing and medical treatment field where protection of individual information and information disclosure are considered

MORIZUMI Tetsuya† KINOSHITA Hirotsugu††
TERATANI Hazuki‡ NAGASE Hiroshi‡

† TOYO NETWORK SYSTEMS CO., LTD. Tsukakoshi,Saiwai-ku,Kawasaki 3–484, Japan
†† Faculty of Engineering,Kanagawa University Rokkakubashi, Kanagawa-ku, Yokohama-si 221–8686, Japan
‡ Kanazawa Institute of Technology 7-1 Ohgigaoka Nonoichi Ishikawa 921 - 8501,Japan

Abstract When the proccssing of information on the nursing medical treatment is systematized, information leakage between communities that compete becomes a problem. Moreover, the leakage of individual information becomes a problem further, too. Therefore, the access control is used as these measures. However, it is necessary to analyze the spread of the content of information, which is not permitted by the access procession, and to control. Because individual information is used in the environment that the social system of nursing and medical treatment, into which the function differentiates operates competing and jointly. Individual information that the social system manages moreover, because of not being falsified the information leakage at all.

This paper describes to apply Community Based Access Control Model for this problem solving in this text, and assumes the proposal of one of the problem solving.

Keyword Nursing medical treatment, Security Model, Access Control, Covert Channel, Web Application System, Social System

1. はじめに

高齢化社会を迎え，介護・医療への関心が高まる中，2000 年 4 月に施行された「介護保険法」に基づいてケアマネージャと言う役割が注目されている．ケアマネージャは介護現場の要的役割を成しており，福祉的社会を円滑化するために重要な位置付けになると思われる．一方，介護・医療の分野に於いても市場原理が導入され，複数の介護福祉施設，病院，関連業者，行政が連携，或いは競合しつつ，患者へのサービスに当たろうとしている．しかし，介護・医療と言う社会システムに於いて産出される情報の中核にはかならず個人情報が含まれる．言い換えれば介護医療は福祉のシステムである．それにも拘らず，介護・医療の提供側は採算を無視できない．即ち，個人情報はその価値がサービスを提供する社会システム側とサービスを受ける家庭側で対立する構造になっている．

そこで，個人情報の漏えい，改ざんを防止し，なおかつ，社会システム側の円滑な競争を促す制御装置を社会システム側に組込む事が求められる事になる．この要求は，介護・医療システムがインターネットで結ばれ，分散化されたデータベースとして機能する事を想定する時必ず満たさねばならない設計要件である．我々は分散データベースをインターネットで接続し，情報漏えいと改ざんを防止しつつ新たな情報を産出するセキュリティモデル“Community Based Access Control Model”と実現システムを研究してきた[16]~[27]．Community Based Access Control Model は，隠れた

情報リークや改ざん（Covert Channel）を分析・制御するアクセス制御のための構造モデルである．本稿では，そのアクセス制御モデルを介護・医療システムに適用する可能性に関して論じる．

2章で競合，連携しつつ情報を産出する機能分化的な社会システムを制御する Community Based Access Control Model が介護・医療の分野にとって必要であると言う着想を，ルーマン社会システム論とハーバーマスのコミュニケーション論をベースに言及する．3章で Community Based Access Control Model について示し，4章でその介護・医療システムへの適用例と効用に関して示す．

2. 介護・医療とアクセス制御の構造モデル

2.1. 介護保険制度

介護・医療制度に関して介護保険業者，ケアマネージャ，費用，介護認定の視点で概観する．

介護保険事業者： 介護保険事業者は個々のサービスの合計に相当する金額の９割を介護保険から支給され，個々のサービスの合計に相当する金額の１割をユーザに請求する．介護保険事業者はケアマネージャを各事業者に置かなければならない．介護保険事業者の種別を以下に示す．

(1)居宅介護支援事業者

利用者の意向をふまえて居宅サービスプランを作成、個々のサービス事業者との調整を行う。（ケアマネージャのみの事業所ではサービス自体は行なわない）

(2)居宅サービス事業者

介護支援事業者と連携して個々のサービスを行う事業者.居宅介護支援事業者と居宅サービス事業者は一体化していることが多い。

(3)介護保険施設.

①介護老人福祉施設（特別養護老人ホーム）：生活介護が中心の施設.

②介護老人保健施設（老健）：介護やリハビリ中心の施設.看護・医学的管理下での介護・機能訓練等.

③介護療養型医療施設：医療が中心の施設収益.

介護保険施設の利用者は保険料の他に食費・居住費・衛生費等を施設に支払う．介護保険施設の本質的な仕組みは介護保険制度を使うという点で共通する．

ケアマネージャ： ケアマネージャは「介護保険法」に基づく役割である。ケアマネージャは要介護者からの相談に応じ、要介護者の介護区分に応じて適切な在宅サービスや施設サービスを利用できる様，市町村、事業者，介護施設との連絡調整を図る．ケアマネージャの主な業務を次に示す．

要介護認定業務

①申請の代行，②認定調査の受託（被保険者宅を訪問調査）

介護支援サービス業務

①課題分析（アセスメント），②介護サービス計画の作成，③サービスの仲介や実施管理，④サービス提供状況の継続的な把握及び評価

給付管理業務

①支給限度額の確認と利用者負担額の計算，②サービス利用票、サービス提供票の作成，③給付管理票の作成と提出

ケアマネージャは各事業者に置かなければならない．

介護保険費： 介護保険費は地方自治体によって金額が異なる．（人口が少ない地域では一人当たりの介護保険費は高くなる）．介護者当たりの介護サービス金額の９割が介護保険費から事業者に支払われる．

高額介護サービス費： 利用者の状態などでやむを得ず１割を超えてしまう場合がある（利用するサービスが多い場合）．利用額限度を超えた額は利用者の実費となり、介護保険事業者に支払われる．上限額を超えた額は高額介護サービス費として，後日市町村から利用者に払い戻される．（市町村に利用者が申請する）．市町村は利用者の払い戻しに応じる．これは事業者にとって利用額限度を超えた額は収入になる事を意味する．そこで市町村は介護保険事業者が利用限度額を超えないサービス計画を立てているかを監督する．介護保険事業者は利用者の上限額を超えない様にサービス計画を立案実行しなければならない．つまり，事業者は高額サービス費の収入を見込んで介護計画を立ててはならない．

介護保険制度に於ける介護認定： 介護認定審査会を市町村が実施する．そのメンバーは，保険・医療・福祉の専門家で構成する．即ち，医師，市職員，アマネージャーが構成員となる．

介護区分： 介護区分は，自立・要支援１・要支援２・要介護１～５，である．介護区分は，区分が高いほど介護保険から病院・施設等へ支給される金額（保険料）が高い．

2.2. 介護・医療の社会システム

介護・医療に，ネットワークとデータベースで構築されたアクセス制御システムを導入することを想定する．この時，アクセス制御システムが必要とする構造モデルを Community Based Access Control Model[21]～[24] に求める．本節では，Community Based Access Control Model が定める関係（属性）の中でも，介護・医療に於いては競合属性とプライベート属性が重要な位置づけになる事を社会システム論的に概観する．

Community Based Access Control Model はルーマン社会システム論[1]，現象学[2][3]，記号学[4][5]をその着想の源としている．ルーマン的社会システムは生物モデルである．即ち，社会システムは環境世界と関係を持つ中で自己を再生産し維持する．環境世界の持つ大きな複雑性を社会システム内部の小さな複雑性へ縮減させる事によって，社会システムは環境世界に反応する．言い換えれば，複雑性は社会システムによって意味の統一と言う機能によって選択され問題解決される．ルーマン社会システムに於ける意味の統一と言う作動は，現象学的概念が導入されたものである．

一方，ハーバーマス[6][7]は，ルーマン社会システム論に於いて“社会が意味を媒介して統合される視点”には賛同したが，“ルーマンの社会システム論にはコミュニケーション的行為による了解のプロセスと，合意の達成と言う概念がない”と批判した．ハーバーマスは現象学的な“主観と客観に関する認識の問題解決の視点”，即ち“主観は決してその外に出られない”と言う視点を社会学に適用する．そこでは主体はコミュニケーションの行為によって共通了解するものとされ，その場所“生活世界”が提唱されている．ハーバーマスは，ルーマンによって消去されてしまった主体を引き戻したと解釈される．

本稿では，現代社会を“貨幣と競争によって成立する機能的に分化したルーマン的社会システム”と想定し，介護・医療分野に於いて，情報へのアクセスを制御すると言う視点に着目する．機能的に分化した社会システムとは，介護・医療・役所・家庭・業者である．これらの社会システムは，競争原理の中でサービスを提供する一方で，個人情報に関係する主体の考え方や個人の権利

を侵害，或いは排除する脅威を持つ．この様な介護・医療システムの行為的目標と主観的な個人（家庭）の意味（価値）に於ける対立は，ルーマンとハーバーマスの論争と根を同じくしている．即ち，介護を受ける側には，認知症を伴う患者の介護を社会的に支援してもらいたい，と言う希望がある一方で，機能分化的な社会は，競争原理に基づいて介護・医療サービスを家庭に提供しようとする．しかし，その介護・医療サービスは，社会システム自身が利益を出して自己を維持できなければ提供する事ができない．そして，この時産出される情報としては，サービス対象としての個人情報の使用が不可欠になる．つまり，個人情報が機能分化的社会システムの情報産出過程の中で不可避的に使用されると言う事である．或いは，個人情報が介護・医療サービスの経営情報と結びつき，競合するサービス提供者に渡ってはならないと言う，社会システム側の自己制約に転化する事も考えられる．

介護・医療サービスと言う社会装置をうまく作動させるためには，ハーバーマスの言う生活世界の中の主体間のコミュニケーション的行為によって，主体の共通了解と言う認識的行為と了解が達成される，とするだけでは不十分である．従って，介護・医療に関わる組織体の情報を処理・制御するメカニズムに関しては，ルーマン的社会システムの概念を導入せざるを得ない．即ち，アクセス制御機能として，社会システムの構造を定め，それに基づいてアクセスを制御するメカニズムを埋め込むというアプローチが必要である．しかし，アクセス制御として提供されるメカニズムは主体（主観）のための道具立てである．そこで，ハーバーマスの言う共通了解的な合意メカニズムを，社会システム間，社会システムと個物としての主体間にバランス良く配置するシステム設計が求められる．即ち，アクセス制御によって，生活世界からの要請を受けたアクセスルールによって個人情報が守られ，かつ，社会システム間の競争を疎外しない社会装置として機能させる事が課題となる．

ルーマンとハーバーマスは社会と言う巨大で複雑な対象を論じる上で論争し，相容れない部分がある．しかし，本稿ではアクセス制御と言う社会装置が作動するための着想を得るために，両者の根元にある思想的構造を導入する事を試みた．即ち，「各社会システムは介護・医療情報を産出する事のみを目的として作動する．そして介護・医療の分野を現象学的に捉え，主体に関しては，同じ主体が複数の機能的に文化した社会システムに帰属する事を想定する．また，介護・医療を受ける主体（患者と家族），提供する主体共々，人間と言う個物は生活世界に帰属し，アクセス制御，及びそれ以外の複雑な意味の解釈と共通了解を実践する」．本稿は，この様な位置付けで介護・医療システムに於けるアクセス制御メカニズムを構築する．

2.3. 介護・医療に於ける知識の構造化とオントロジーのアクセス制御への適用

■知識の構造化

知識を構造化するには，知識が厳密に定義され，関係者が合意する概念（用語）が必要となる．そして，構造化された概念によって，様々な現象，観測事象，興味ある対象が新たに産出，或いは再生産される．この様な操作によってできる概念間の関係は意味ネットで表現される．オントロジーはその様な意味ネットに於いて知識を構造化し，推論する機能として位置付けられる．

また，知識の中には階層化されずに半構造的に結びつく様な範疇に属するものもある．このような知識を表現するツールとしても意味ネットが使用される．

■データ構造

データベースの概念スキーマはデータベースのオントロジーであるが，その視点に於いてオントロジーに基づいた意味ネットは対象世界に存在する概念や情報を記述するデータ構造を提供する．また半構造的なデータ構造を導入する事によって，必ずしも合意に至っていない概念的な思考やレトリックを表現する事が可能になる．

■セキュリティモデル[8]~[15]の位置づけ

オントロジーはある対象をモデル化するときに必要となる概念とそれらの間に成立する関係を明示的に規定する．即ち，対象のモデルはオントロジーが提供する概念と制約の下で作られる抽象化されたモデルである．

一方，セキュリティモデルは現実対象を抽象化して主体が客体にアクセスする事を制御する構造モデルである．即ち，セキュリティモデルをオントロジーとして見ると，データベースの概念スキーマに加えて，主体と客体のアクセスを構造的に関係付けたモデルであると言える．この構造化の過程に於いて，主体自身の情報産出に対する構造が明確化される．例えば，社会に於ける主体の役割，だれが客体を産出したか，或いは，主体自身の情報，と言う意味が反映された構造である．

更に，セキュリティモデルで使用するアクセス権限に対する制約（アクセスルール）や，アクセスされる客体のアクセス状況は，それらを変更すると言う現実的な要求を満たす必要がある．従って,セキュリティモデルの位置づけは,メタ知識と言う固定的で形式的なモデルとせずに，“知識状態”と“知識状態の遷移”と言う構造として捉える事とする．

■セキュリティモデルの属性とアクセスルール

オントロジーでは概念間の意味定義（制約）や関係の記述（公理的記述）によって，オントロジーで構築された概念スキーマの構造を与えると共に，オントロジーを用いて記述されるもの全体の性質に関する質問に答える．

セキュリティモデルの概念スキーマとは，主体客体が社会システムの中で刻印される属性とそれに基づいたアクセス関係である．属性とは，競合属性，階層属性，役割属性，所有属性，プライベート属性である．

セキュリティモデルの概念スキーマはデータ構造と密接に関係する．即ち，客体へのアクセス許可，不許可，或いは，客体の記号内容部の漏えいや改ざんを防止する手段の妥当性を推論するために，客体が持つオントロジーや意味ネットの構造と主体の属性を利用する．言い換えれば，主体と客体の属性を明確に定義出来てこそ，Covert Channel かどうかを自動的に推論でき，情報フィルタとしてパミッションをどう変更するかと言う推論が可能になる．

2.4. セキュリティモデル概要

セキュリティモデルは，アクセス制御の視点から実世界を捉えた構造モデルである．構造モデルは要素と関係から成る．セキュリティモデルの要素はアクセス行為の主体とアクセスされる客体である．セキュリティモデルの関係は，社会シス

テムから主体と客体に刻印される属性，主体自身が持つ性質としての属性，そして客体が持つ意味の関連性を示す属性である．主体と客体が属性を持ち寄ってコミュニティができる．コミュニティは社会システムである．主体の主観は生活世界の中にあり，コミュニティへの帰属は社会システムに帰属する属性に基づく．例えば，ある人は家庭を持ち，会社Aの社員であると同時に，政府機関協議会の委員である,と言う様に,複数のコミュニティに役割を持って参画する．主体・客体・コミュニティ・属性によって構造的に表現された社会システムに基づいて，主体が客体にアクセスする行為に制約を設けたものがセキュリティモデルである．アクセス行為の制約はルールとして表現される．要素，関係，ルールを知識状態と呼ぶ．知識状態は，ルールの変更・追加，アクセス要求に応じて状態遷移する．セキュリティモデルによる制御目的は，知識状態が Covert Channel を分析・制御された状態である事を保証する事である．

2.5. アクセストリプルと Covert Channel

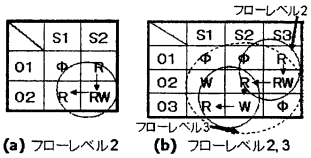
主体，客体，パミッションからなるアクセストリプルの集合，“アクセス行列”に於いて，Covert Channel を定義する．

【定義】 Covert Channel: アクセス行列において、アクセス禁止のパミッションに矛盾する情報フローを Covert Channel と呼ぶ．即ち，主体 Si(i＝1, 2, ･･･), Sj(j＝1, 2, ･･･),但しi≠j, 客体 On(n＝1, 2, ･･･), Om(m＝1, 2, ･･･), 但し n≠m, パミッション P{RW, ¬RW, ¬WR, ¬(RW)},但し, R(READ),W(WRITE)とする時，アクセストリプル<Si,On,P＞について，

If <Si,On,¬R>,
And if <Sj,On,R>∧<Sj,Om,W>∧<Si,Om,R>,
Then CovertChannel(Si,Sj,Om(On)).

と定義する．

この定義では，主体 Si は客体 On と言う記号作用部とその記号意味部(内容)を READ 禁止<Si,On,¬R>であるにも拘わらず，主体 Sj が客体 On の記号意味部を READ し，客体 Om に WRITE し，主体 Si が Om の記号意味部から客体 On の記号意味部を READ する事(<Si,On,R>と表現される)によって，アクセストリプル<Si,On,¬R>と矛盾する結果が生じる事が示される．図1(a)に CovertChannel (S1, S2, O2(O1))を示す．また，Covert Channel が引き起こされる時，それに関わる主体の数によって Covert Channel の程度(フローレベル)を定義する．



(a) フローレベル2　(b) フローレベル2,3

図 1 Covert Channel とフローレベル

【定義】フローレベル: Covert Channel に関わる主体の数をフローレベルと呼ぶ．

3. Community Based Access Control Model

3.1. 要素の定義

主体，客体，パミッション，コミュニティ

コミュニティの定義を次に示す．

【定義】客体: 客体は，データベースに格納される情報である．客体は，そのタイトル，及び，その内容から成る．

【定義】主体: 主体は，客体にアクセスして操作する実体である．

【定義】コミュニティ: コミュニティは，そこに帰属する主体の属性，客体の属性の集まりである．

3.2. 属性の定義

■社会システムの視点に於ける属性

【定義】競合: コミュニティ間の関係であり，競合関係にあるコミュニティどうしはアクセスが禁止されなければならない．

【定義】役割: コミュニティが主体に刻印する関係．コミュニティ内の情報産出機能に関わる．

【定義】階層: 主体，客体に刻印されるセキュリティ・レベル．

【定義】所有: 客体の所有を示す属性．

■生活世界の視点に於ける属性

【定義】プライベート: 個物としての主体は，主体自体に関わる情報を持つ．この情報の属性をプライベートと呼ぶ．

■意味の構造により分類される客体の属性

Eを記号作用部，Rを関係，Cを記号意味内容部とし，ERCを客体を記号として意味まで表記する最小単位とする．{ERC}を(ERC)の集合とする．

【定義】メタ言語属性とレトリック属性:

(1) メタ言語 ER{(ERC)}: Eは概念を名詞化した言葉，{(ERC)}は概念Eを言葉で説明した内容を象徴的に表現した内容であり，この関係をメタ言語と呼ぶ．

(2) レトリック{ER{(ERC)}}RC:メタ言語集合{ER{(ERC)}}と判示的な内容 C の関係をレトリックと呼ぶ．

3.3. 権限の譲渡，利用

主体，客体，およびそれらに固有の属性に基づいて，主体と客体の2項関係からパミッションを分析，制御する構造に加えて，アクセス権限自体を譲渡する，或いは，利用を許可すると言う構造を導入する．そのためのメカニズムは take-grant モデルの概念[12][13]を導入し，権限を受ける要求 take と権限を渡す要求 grant が対になるイベントが発生した時，該当するアクセス権限のやり取りが実行され，知識状態が遷移する．属性に対する take-grant のはたらきを次に示す．

(1) 情報産出が社会システムの基本的機能であるので，情報産出過程に於いて定まる競合属性は社会システム固有のものであり，譲渡の対象にはなり得ない．

(2) 階層属性,役割属性は，特定の社会システムの規範によって決定されるものである．従って，Community Based Access Control Model では譲渡ではなく，アクセス行列の変更と見做す．

(3) Private属性は個人情報に関わり，その譲渡は有り得ない．しかし，社会システムに対し，利用を許可する．

(4) 所有属性はローカルな譲渡が可能である．

3.4. アクセスルール

アクセス要求，及びコミュニティに於ける情報フローが Covert Channel であるかどうかを判定するためにアクセスルールを規定する．更に，Covert Channel と判定された情報フローを修正し，或いは修正が不可能の場合はアクセスを禁止するフィルタ処理を行なうフィルタルールを規定する．アクセスルールとフィルタルールを指す場合をルールと呼ぶ．

ルールはコミュニティ，主体，客体の構造として定義された属性，即ち関係とアクセス行為が矛盾しない様に規定される．２つの属性集合 ξ，η をコミュニティ，主体，客体の属性の任意の組合せであるとし，アクセス規則を適用するための比

較を ξ.R.η （.R.は２項関係を表す）とする時，属性ξ，ηを比較し，真偽を推論するための基本的なルールを次に示す．

■属性の単独ルール

［競合属性］

(R1) ξとηがそれぞれコミュニティ名属性と役割属性の組合せを含み，かつそれらが競合関係であるならば，ξ.R.ηに於いて競合属性間のアクセスが禁止される．

[役割属性]

(R2) ξまたはηが役割属性を含む時，あらかじめ定めた役割属性のパミッションと矛盾がなければアクセスを許可する．

[階層属性]

(R3) ξが階層属性（セキュリティレベル）を含み，ηが階層属性を含まない時，かつ，セキュリティレベルが機密性を目的とするならば，ξ.R.ηによってξの階層属性からηへの客体流出が禁止される．

(R4) ξが階層属性（セキュリティレベル）を含み，ηが階層属性を含まない時，かつ，セキュリティレベルがインテグリティを目的とするならば，ξ.R.ηによってξの階層属性からηへの客体流入が禁止される．

[所有属性]

(R5) ξ.R.ηの一方，ηが所有属性を含む時，ηはξからのWRITEが禁止される．

(R6) ξ.R.ηが所有属性を含み，所有関係に矛盾がない時，ξはηへWRITE可能である．

(R7) 所有属性に対するREADのアクセスは，競合属性，階層属性に従う．

［プライベート属性］

(R8) ξ.R.ηに於いて，ξとηが同一のプライベート属性の値を持つ時，ξ.R.ηのアクセスが許可される．

(R9) ξ.R.ηの一方がプライベート属性を含む時，プライベート属性を持つ客体へのアクセスが禁止される．

(R10) ξ.R.ηの一方がプライベート属性を含む時，プライベート属性にアクセス許可された主体に限り，アクセスが許可される．

■属性間のアクセスルール

(R11) 競合属性はアクセスの判定全てに優先する．

(R12) ξ.R.ηの少なくとも一方が役割属性と階層属性を２つ同時に含む時，ξ，η間のアクセスルールは階層属性のルールに従う．

(R13) ξ.R.ηの少なくとも一方が所有属性を含む時，{(R11)(R12)}のルールの下で所有属性のルールに従う．

(R14) ξ.R.ηの少なくとも一方がプライベート属性を含む時，{(R11)(R12)}のルールの下でプライベート属性のルールに従う．

3.5. 構造モデルに基づく安全性の分析・制御

コミュニティが安全であるとは，Covert Channelが分析・制御されている状態であるとする．この状態を知識状態として，遷移した状態を分析する妥当性の根拠とする．アクセス制御を司るコミュニティはルーマン的社会システムの性質を受け継ぎ，自らのみの制御と言う情報産出を実行する．他のコミュニティについては外部環境であり内部は不明である．しかし外部コミュニティとの共通領域を設け，アクセストリプルのコミュニケーションを行い，安全性の分析・制御を継続的に実行する．安全性の判断は，ある時点で安全性が満足されている知識状態から推論する．以下に詳細を示す．

[1] 知識状態 σ_k

知識状態 σ_k とは，ある認識史の時点kに於ける，要素 EL_k，属性(関係) AT_k，パミッション PA_k，ルール RU_k の直積である．

$$\sigma_k = EL_k \times AT_k \times PA_k \times RU_k$$

[2]知識状態への入力イベント

i,k,m,n を自然数とする．知識状態 σ_k への入力イベントは，次の2種である．

(1) アクセス要求 $e_k \times a_k \times p_k$ ，$e_k \in EL_k$, $a_k \in AT_k$, $p_k \in PA_k$

(2) アクセスルール，フィルタルールの追加変更

[3]知識状態 σ_{k+1} の安全性分析・制御

(1) 時点kの知識状態が σ_k のもとでコミュニティが安全である必要条件は，Covert Channelが防止されている状態である．

(2) 時点kの状態に入力イベントが発生すると，知識状態は σ_{k-1} になる．この時，σ_{k-1} が σ_k から矛盾無く推移するならば，知識状態 σ_{k-1} に於いてもCovert Channelが防止されている，とする．

(3) σ_{k+1} が σ_k から矛盾無く推移するための必要十分条件は，知識状態 σ_k に於いて，ルール RU_k によってCovert Channelを推論し，かつフィルタを作動させる事である．

[4]コミュニティごとに異なる知識状態の安全性

コミュニティnの時点kに於ける知識状態を σ^n_k とする．

$$\sigma^n_k = EL^n_k \times AT^n_k \times PA^n_k \times RU^n_k$$

(1) コミュニティnは，自身以外の外部コミュニティの知識状態の全てを知り得ない．

(2) コミュニティnはイベントとして外部コミュニティmとアクセス要求を交換し，外部コミュニティmのアクセス要求 $e^m_k \times a^m_k \times p^m_k$ を元に新たな知識状態 σ^n_{k+1} とする．

$$\sigma^n_{k-1} = (e^m_k \vee EL^n_k) \times (a^m_k \vee AT^n_k) \times (p^m_k \vee PA^n_k) \times RU^n_k$$

e^m_k, a^m_k, p^m_k は外部コミュニティmとの共通領域となる．

(3) コミュニティnは時点k+1の新たな知識状態 σ^n_{k+1} に於いて安全性分析・制御[1]を実行する．

4. 介護・医療システムへの適用と推論機能

4.1. 介護・医療システムの行為的目標と主観的な個人(家庭)の対立構造

介護・医療システムに於いて想定する組織体を，病院，介護施設，ケアマネージャ事務所，建設業者・介護用品販売業者，要介護者とその家庭，役所とする．これらの介護・医療の行為的目標と個人（家庭）の対立構造は次の様な項目が考えられる．

■病院

・病院どうしは経営上，競合している．
・他の病院に対して，要介護に関する医師の判断基準に関する情報を公開したくない．
・要介護患者情報は病院の経営情報に関係する．
・介護レベル４，５の患者を入院させたい．
・要介護に関する意見書を医師が書くことができる．
・病院のMedical Social Workerは要介護情報や患者家族情報を取り扱う．
・Medical Social Worker (MSW)役所，ケアマネージャと介護認定委員会で情報をやりとりする．
・介護施設と連携する場合がある．
・介護レベル３以下は介護施設に入所してもらいたい．

■介護施設

・病院から患者を照会してもらいたい．
・介護レベル４，５，かつ治療を必要としない患者を入所させたい．
・他の施設に対して，介護諸費用に関する情報を公開したくない．
・ケアマネージャは，要介護情報や患者家族情報を取り扱う．

■ケアマネージャ事務所

・ケアマネージャは，要介護情報や患者家族情報を取り扱う．
・ケアマネージャは，要介護患者の家庭に対して介護用品業者や家屋リフォーム建設業者を斡旋する．

■建設業者・介護用品販売業者

・できるだけ多くの要介護家庭と言う市場を発掘したい．
・病院，介護施設・ケアマネージャ施設から家庭を紹介してもらいたい．

■要介護者とその家庭

・できるだけ安価で，かつ，サービスの良い施設，病院へ入所させたい．
・早く患者を入所させたい．
・介護レベルを下げられて退院させたくない．
・家庭内で介護したい．

次に上記の例に関して介護・医療システムが個人情報におよぼす脅威を示す．
(1)要介護認定委員会
・医者，役所の介護担当,ケアマネージャ（或いは病院の MSW）をメンバーとする“要介護認定委員会”，“入所判定委員会”が開催され，患者の介護度が認定される．これら委員会は想定した組織体共々コミュニティであり，利害が錯綜する場所となる．
(2)個人情報は，事業所のスタッフの大半は閲覧可能．
(3)事業所間の繋がりもあり，個人情報がやり取りされる．
(4)居宅の場合、ケアマネージャは自宅に入り込むため家庭環境や預貯金等の情報が分かる．
(5)サービスを提供していないのに提供したかのように事業者が申請して保険料を騙し取る．
(6)介護医療製品業者，リフォーム業者が設備や備品供給者として加わる．

また，介護・医療システムでは患者を元にした競合と連携の関係があり，各コミュニティからの情報漏えいがコミュニティにとって不利益になる事を防止しなければならない．

4.2. 介護・医療システムのコミュニティ，主体，客体

介護・医療システムに Community Based Access Control Model を適用し，そのはたらきと効果を示す．一例として次の様なシステムを想定する．

介護・医療システムに於ける役割

R1:ケアマネージャ	介護施設
R3:一般介護管理者	介護施設
R5:介護認定審査会メンバー	介護認定審査会
R6:介護担当職員	役所
R7:介護課管理者	役所
R8:医師	病院
R9:MSW	病院
R10:業者	介護用品(株)

介護・医療システムに於けるコミュニティと役割

介護施設:Com_Nr1	R1,R3
介護施設:Com_Nr2	R1,R3
ケアマネージャ事務所: Com_Co1	R1
病院:Com_Mc_1	R8,R9
役所:Com_Po1	R6,R7
介護認定審査会: Com_Comrec_1	R5,R1,R6,R8,R9
要介護者とその家庭: Com_Fam	S1
建設業者・介護用品販売業者:Com_Tr	R10

主体 Si(i は自然数)と役割の対応: [S2:R1,R5], [S3:R5], [S4:R6,R5], [S5:R8,R5], [S6:R9,R5]

コミュニティの競合関係

介護施設:Com_Nr1 ⇔介護施設:Com_Nr2
ケアマネージャ事務所:Com_Co1⇔介護施設:Com_Nr2

客体を作成する役割

(O1:ケアプラン原案)	ケアマネージャ
(O2:介護サービス計画書)	ケアマネージャ
(O3:サービス申込書)	ケアマネージャ
(O4:介護保険要介護認定・更新申請書)	ケアマネージャ
(O5:主治医意見書)	医者
(O6:介護認定審査会資料)	ケアマネージャ,介護担当職員,医者,MSW
(O7:介護用品保守打合せ資料	ケアマネージャ,一般介護職員,MSW

客体の記号意味部

Cp: 患者の氏名，生年月日，住所，性別情報．
Cl: 要介護区分．
Cl1: 現在の要介護度．
Cl2: 現在の要介護度の有効期間．
Cs: 病歴
Cf: 家族の有無や構成．
Ch: 家の構造．
Cv: 認定判断の記録
Ce: 介護設備保守情報

客体の記号作用部と記号意味部

(O1:ケアプラン原案) R {Cp, Cl, Cs, Cf, Ch,Cu}
(O2:介護サービス計画書) R {Cp, Cl}
(O3:サービス申込書) R {Cp, Cs, Cf }
(O4:介護保険要介護認定・更新申請書) R {Cp, Ch}
(O5:主治医意見書) R {Cp,ClCs}
(O6:介護認定審査会資料) R {Cp, Cl,Cu, Cv}
(O7:介護用品保守打合せ資料 R {Ce})

システムに於いて保護する客体は，個人情報であるとする．即ち，次の5つである．
1. 被保険者の氏名，生年月日，性別，住所，電話番号
2. 家族構成
3. 本人の健康状態
4. 家屋の見取り図や状況
5. 家族の氏名，生年月日，性別，住所，電話番号

介護・医療システム例のアクセス行列

4.3. 競合．役割・プライベート属性と Covert Channel

図2に介護・医療システム例(4.2 節)のアクセス行列を示す．図2から，介護・医療システムに於ける競合属性，役割属性，プライベート属性に関して，Covert Channel が如何に引き起こされているか,それに対してどのようにアクセスルールを適用するかを示す．

コミュニティ内の個人情報漏えい:

■コミュニティCom_Nr1 の中にあって，役割 R1 と役割 R3 の間には，客体 O2 を介する Covert Channel によって客体 O4 が R3 に情報漏えいする．
■コミュニティCom_Nr1 の中にあって，役割 R1 と役割 R3 の間には，客体 O2 を介する Covert Channel によって R1 は客体 O7を間接的に情報改ざん可能である．
[ルールの適用]: プライベート属性ルール(R13)を満たす様にパミッションの変更等を実施し，知識状態を安全状態にする．

コミュニティ間の連携的な個人情報の漏えい:

■コミュニティCom_Nr1 の役割 R3 はコミュニティCom_Tr の役割 R10 に対して客体 O2 につき，客体 O7 を介する Covert Channel によって情報漏えいさせる事ができる．
■コミュニティCom_Nr1 の主体 S2 は役割 R1 を使いコミュニティCom_Nr1 の客体へのアクセス権限がないコミュニティCom_Co1 の役割 R1 に対して，客体 Oξを介する Covert Channel によって情報をリークさせる事が可能である．
■主体 S2 はコミュニティ Com_Nr_1 と Com_Comrec_1 に帰属し，それぞれ役割 R1 と R5 を持つ．もし主体 S2 が自分用 PCに Com_Nr_1 の客体をそのままコピーしていれば，役割 R5 に於ける O1,O2,O3 へのアクセス禁止は効果が無く，S2 は客体 Oξを介して業者 Com_Tr に当該客体を Covert Channel 或いは直接的に転送可能となる．
[ルールの適用]: プライベート属性ルール(R13)を満たす様にパミッションの変更等を実施し，知識状態を安全状態にする．

競合するコミュニティへの個人情報漏えい:

■主体 S2 はコミュニティ Com_Comrec_1 の R5 の役割と，Com_Nr2 の R5 の役割を持つので，Com_Nr2 の O4 に対して主体 S2 は役割 R5 を利用して直接 READ 可能である．
■もし，コミュニティ Com_Comrec_1 の役割 R5 が，異なる主体 S3 と S2 の役割の時，Com_Nr2 の O4 の Ch 即ち家の構造が Covert Channel によって，競合するコミュニティCom_Nr1の O6 に漏えいする．
[ルールの適用]: 属性間のアクセスのルールの競合属性のルール (R11)を適用し，パミッションの変更等を実施して知識状態を安全状態にする．

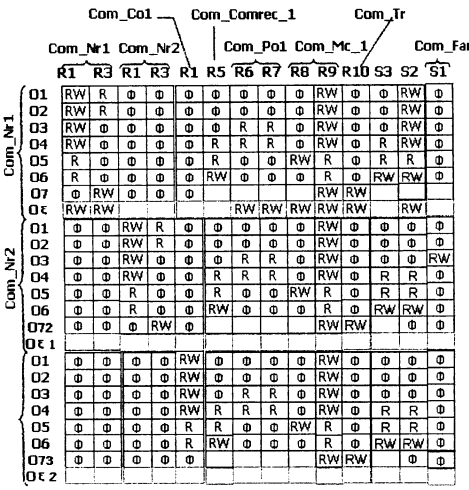


図2 介護・医療システムのアクセス行列

図2に見られる様に，介護・医療システムに於ける脅威は，コミュニティ（社会システム）の情報産出活動に不可欠な要素としての個人情報に関わる脅威と，競合関係に関わらず，生活世界の個人情報がシステムの不備によって社会に拡散してしまう脅威の2つである．これらの場合に対して，セキュリティモデルは情報漏えい・情報改ざんを防止するために次の様な制御効果を発揮する．

（1）コミュニティの活動がもたらす個人情報の脅威への対抗策

介護・医療で用いる情報は，ビジネス的視点に於いて個人情報の属性を持つ情報が直接経営に利用される．この時，競合関係のルール(R1)(R11)により，競合関係にあるコミュニティへのCovert Channelは禁止フローとして抽出される．或いは，コミュニティ同士の連携関係としてプライベート属性の客体が伝播される場合，プライベート属性のルール(R8)(R9)(R10)(R14)によって制限される．役割属性とプライベート情報が組合されている場合，ルール(R10)によりプライベート属性が優先され，個人情報の伝播が防止される．ルールは無制限のプライベート情報の伝播を制限している．

（2）システムの不備による個人情報漏えいの脅威への対抗策

介護・医療システムでは，使用する客体の全てにプライベート属性が含まれる．従って，役割属性が刻印された客体からそれがない客体 Oξへのread,writeによってたやすくCovert Channelが生じる．また，コミュニティ“介護認定審査会Com_Comrec_1”は，そのメンバーとしての役割“ケアマネージャ”，“介護担当職員”，“医師”，“Medical Social Worker”の帰属が規定されている．そして，これらの役割を持つ主体は“介護認定審査会メンバー”と言う役割を重複して持ち，かつ異なるコミュニティに帰属している．この構造がCovert Channelの一因となる．即ち，これは異なるコミュニティに帰属し同じ役割を持った主体が一堂に会すコミュニティがある場合にCovert Channelに注意しなければならない事を意味する．

この様な問題に対して，セキュリティモデルはCovert Channel分析を行い，その結果をルールに基づいて推論し，Covert Channelを防止する対策（パミッションの変更等）を実行する．プライベート属性はルール(R8)(R9)(R10)(R14)に基づいて分析される．

4.4. セマンティックWeb技術の適用可能性

4.4.1 知識状態σkの分析推論機能

Community Based Access Control Modelは，アクセス制御に必要なセキュリティポリシーの枠組みを社会システム的な構造から抽出し，それに基づいて直接的なアクセス，及びCovert Channelを引き起こす情報伝播経路の推論を実行するシステムである．そのためには，アクセスのルールの枠組みをベースとして個々のコミュニティのルールを記述しそれに基づく推論を行なう“論理型言語による推論機能”が必要になる．また，データベースへのアクセスを制御するのであるから，データの意味を記述し，不完全な意味ネットであってもセキュリティモデルの構造とデータの意味の構造から推論する“意味ネットによる推論機能”が必要である．この様な意味ネットとその意味を推論するシステムとして，オントロジー言語OWL，RDF(Resource Description Language)等，セマンティックWeb技術の適用が有望である．即ち，セマンティックWebはインターネットを介して分散するデータベースへの情報の意味論的検索機能を実現するものであると見做せるが，そのデータへのアクセス制御そのものがCommunity Based Access Control Modelの機能である．

4.4.2 アクセス行列のブランクの推論

意味ネットのアプローチとアクセス制御の接点として，アクセス行列の要素（パミッション）が完全に埋まっていない場合，それでもCovert Channelを分析する機能に関して述べる．

【パミッションのブランク処理1】

アクセス禁止パミッションを持つアクセストリプル<Sk.Ok, Φ>に関して別のトリプル<Si,Ok,RW>があり，そのOkが客体Ojに WRITEされた時，Ojを RW 可能な主体 Siのパミッションがブランクであるならば，<Si,Ok,R>と仮定し，フローレベル2を検出する．但し，<Si,Ok,R>と仮定する事がコミュニティ，主体，客体の属性関係に矛盾しない事が前提である．この推論のためにアクセスのルールを適用する．

図3にブランク対応のダイナミックな処理例を示す．S1がO1をREADしO2に内容をWRITEした時<S2,O2,R>と記される(図3(1))．図3(1)をフローレベル2分析するとこの場合は Covert Channelである事が分かる．

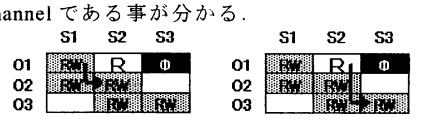


図3 ブランク対応のダイナミックな処理

この場合，O2への WRITEがあった段階で<S2,O3,Φ>とパミッション変更する，この様にクリティカルな情報フローが生じた段階で情報フィルタを掛けると言う処理により，パミッションの変更が多数箇所に及ばなくなり，使い勝手が向上する．

【パミッションのブランク処理２】
パミッションがブランクとなる場合，これをアクセス禁止と見做す場合もある．しかし，この方法は使い勝手を悪くする．この時，フローレベル２の Covert Channel 分析をする前処理として，客体のメタ言語構造，或いはレトリック構造からブランクのパミッションを推論する．ここに，客体の構造(ERC)を導入したメリットが生かされる．

簡単な例を図４に示す．図４は，メタ言語 O2 R {O3,O4}の場合を示す．

	S1	S2
O1	RW	Φ
O2	RW	RW
O3	RW	
O4	RW	

図４　客体の意味の構造に基づくブランク推論

メタ言語はその下部構造として O3,O4 を持つ．そして，メタ言語 O2 の意味にはメタ言語 O3,O4 の意味が含まれている．即ち，O2,O3,O4 はそれぞれメタ言語のタイトルであるが，その内容はまた別に有り，ユーザは O2 から O3,O4 の内容を推論可能な場合があり得る．そこで，システムのアクセスルールとして“メタ言語タイトルのパミッションは下位構造のメタ言語タイトルに継承される”，と規定する事によってアクセス行列のブランクを埋める．次に埋められたパミッションに基づいて Covert Channel 分析し，アクセスのルールによって Covert Channel を推論する．

5.　むすび

機能分化的社会システムを制御する Community Based Access Control Model が介護・医療の分野にとって必要であると言う着想を，ルーマン社会システム論とハーバーマスのコミュニケーション論をベースに言及し，Community Based Access Control Model の介護・医療システムへの適用例と効用に関して示した．

介護・医療システムに於いて，役割（role）を決め，書類を役割ごとにアクセス権限を定めてもなお,Covert Channel が起こり，情報漏えい，情報改ざんが引き起こされる．介護・医療システムに特有で深刻な事態は，ケアマネージャの様なアクセス権限が集中する役割がある点である．その様な役割に対する攻撃，或いは歪が個人情報漏えいを引き起こし，システム崩壊に繋がる．また，役割と客体の設計が完全であっても，現代社会では役割を担っている主体の役割が多義に渡り，コミュニティへの帰属も１つではない．これも Covert Channel の原因となる

この様な問題に対して，性悪説とはまた異なる概念に基づき，役割を担い，かつ生活世界の場所にいる主体の存在を認めた上でシステム要件を抽出する事は意味があると考える．主観の良し悪しを議論するのではなく，またシステムを硬直化させる制約指向的システムでもない，即ち，情報の産出には複数の主体が関わりあうと言う構造を考慮に入れた Community Based Access Control Model を導入する効果が期待される．

文献

(1) 二クラス・ルーマン(著)，馬場靖雄(訳)，:“ルーマンの社会理論”，勁草書房.
(2) 竹田青嗣:“現象学入門”，NHKブックス.
(3) 斉藤慶典:“思考の臨界－超越論的現象学の徹底”，勁草書房,(2001).
(4) ロラン・バルト，佐藤信夫(訳) :“モードの体系”，みすず書房.
(5) R・カワード，J・エリス(磯谷孝(訳)):“記号学と主体の思想-バルト・ラカン・デリダ・クリステヴァなど”,誠信書房.
(6) ユルゲン・ハーバーマス:“近代の哲学的ディスクルス”，岩波書店.
(7) 小牧 治，村上隆夫:“ハーバーマス”，清水書院.
(8) National Computer Security Center : “A GUIDE TO UNDERSTANDING COVERT CHANNEL ANALYSIS OF TRUSTED SYSTEMS”, NCSC-TG-030, Library No. S-240, 572, Version 1, Nov., 1993.
(9) D.E. Bell, L.J. LaPadula : “Secure Computer System : Unified Exposition and Multics Interpretation”, MI-TRE, MTR-2997, 1976.
(10) MORIZUMI Tetsuya, TUJII Shigeo: “ On the Security Model Based on Lattice-Ordered Groups ”, 1993 KOREA-JAPAN Joint Workshop
(11) D.F.C. Brewer, M.J. Nash : “The Chinese Wall Security Policy”, IEEE Symp. On Security and Privacy, pp.206-214. 1989.
(12) R.S. Sandhu, M.E. Share : ”Some Owner Based Schemes with Dynamic Groups in the Schematic Protection Model”, IEEE Symposium on Security and Privacy, (1986).
(13) L. Synder : “Formal Models of Capability-Based Protection Systems”, IEEE Trans., Compt., Vol. C-30, No.3, pp.172-181, Mar., 1981.
(14) ”Role Based Access Control”, ANSI , INCITS359-2004 (approved 19 Feb 04).
(15) MORIZUMI Tetsuya(ATR),NAGASE Hiroshi (ATR),TAKENAKA Toyofumi (ATR),YAMASHITA Kouichi (ATR) : “ An Evaluation of Security Requirements Based on the Capability Model ”, IEICE Transactions, Vol.E74, No.8, AUG. (1991).
(16) 牛頭靖幸、森住哲也、稲積泰宏、木下宏揚、:“Covert Channel 分析評価のためのアクセス制御エージェントシステムの提案” コンピュータセキュリティシンポジウム 2004、(2004.10.20～22).
(17) 森住哲也、牛頭靖幸、畔上昭司、酒井剛典、稲積泰宏、木下宏揚、小柳和子 : “アクセス制御エージェントシステムによる安心・安全なWebアプリケーションシステム”、 学際的情報セキュリティ総合科学シンポジウム、2004.11.22～23、(2004).
(18) 森住哲也、牛頭靖幸、畔上昭司、酒井剛典、稲積泰宏、木下宏揚 :“セマンティック Web システムにおける“Community Based Access Control Model ”の適用に関する一考察”, SCIS2005,3B1-4, (2005).
(19) 酒井剛典、森住哲也、牛頭靖幸、畔上昭司、稲積泰宏、木下宏揚 ,:“Web アプリケーションシステムに適したセキュリティモデル“Community Based Access Control Model ”の提案”, SCIS2005, 3B1-5,(2005).
(20) 森住哲也、牛頭靖幸、稲積泰宏、木下宏揚:“Covert Channel 分析評価のための Access Control Agent System の提案”, JSSM 論文誌,(2005).
(21) 森住哲也、木下宏揚 :“セマンティックWebシステムのセキュリティモデル”,技術と社会・倫理研究会,(2005).
(22) 森住哲也、木下宏揚 :“社会システムの中の Covert Channel について”,技術と社会・倫理研究会,(2005).
(23) 森住哲也，酒井剛典，畔上昭司，稲積泰宏，木下宏揚:“機能分化的社会システムの属性に基づくセキュリティモデル”，技術と社会・倫理研究会， (2005).
(24) 森住哲也，木下宏揚:“インターネット社会の情報漏えいを防止するセキュリティモデルの提案(社会システム論と記号学からの着想)”，第 2 回情報セキュリティ学際シンポジウム, (2005).
(25) 酒井剛典,森住哲也,畔上昭司,小松充史,稲積泰宏,木下宏揚:“Covert Channel 分析メカニズムと EJB による情報フィルタの構築” ,SCIS2006,(2006).
(26) 畔上昭司,森住哲也,酒井剛典,小松充史,稲積泰宏,木下宏揚:“形式的仕様記述言語 CafeOBJ による Community Based Access Control Model の評価” ,SCIS2006,(2006).
(27) 小松充史,森住哲也,酒井剛典,畔上昭司,稲積泰宏,木下宏揚:“関係データベース，XML データベースに於ける Covert Channel の解析と情報フィルタの構成について”,SCIS2006,(2006).