情報処理学会研究報告
IPSJ SIG Technical Report

Vol.2009-CSEC-46 No.36
2009/7/3

セキュリティラベルの仮名化による安全な情報フロー制御システム連係の実現

樋口直志[†1]　本田篤史[†1]
朝倉義晴[†1]　才田好則[†1]

複数の動的情報フロー制御系間で情報を交換する際には，情報にセキュリティラベルを付随させる必要がある．その場合，情報そのものだけではなく，セキュリティラベルを介しても情報漏洩が生じる危険性がある．そのような情報漏洩を防止するために，我々は，セキュリティラベルを仮名化する手法を提案する．この手法により，セキュリティラベルの不当な照合や，改竄による情報漏洩を防止できる．

Security-label pseudonymization for secure interaction between infomation-flow control systems.

Naoshi Higuchi,[†1] Atsushi Honda,[†1]
Yoshiharu Asakura[†1] and Yoshinori Saida[†1]

To make communication between information processing systems under information flow control, Security-labels must be attached to communicated information. In such case, confidential information may leak not only through the communicated information itself, but through its security-label. To prevent confidential information from leaking via security-label, we propose a method for aliasing security-label. By this method, confidential information is prevented from leakage by cross checking security-labels in conspiracy or falsificating security-label.

†1 日本電気株式会社 システムプラットフォーム研究所
System Platforms Research Laboratories, NEC Corporation.

1. 序　　論

多段階の情報処理を伴う情報システムにおいて、情報の伝播範囲を制御し、機密性・完全性を保つために情報フロー制御技術が研究されている。情報フローとは、情報の演算と転送に起因して、情報が別の情報の値に影響を与えることを指す[1)]。

また、情報フロー制御技術の一種として，実行時情報を反映した制御を行う動的情報フロー制御技術が提案されている[2)]．この方式では，情報システムが取り扱う個々の情報に，セキュリティラベルと呼ばれる分類子を付随させ，情報伝播の可否を実行時に判定する．

このような動的情報フロー制御技術に制御された情報システム (動的情報フロー制御系) を複数連係させる場合には，セキュリティラベルを介してメタ情報が漏洩する危険性がある．まず，情報システムの連係においては，情報がシステム間で交換される．かつ，動的情報フロー制御系では情報にセキュリティラベルを付随させる．そのため，動的情報フロー制御系の連係においては，セキュリティラベルも情報と共に交換される．ここで，セキュリティラベルは，情報生成源の識別情報といったセキュリティ上重要なメタ情報を含むので，取り扱いに注意を要する．例えば，給与額情報に個人を識別できるセキュリティラベルが付随する場合，給与額という情報そのものだけでなく,「誰の」給与なのかというメタ情報も交換される．しかしながら，従来の動的情報フロー制御系では，システム間のセキュリティラベル交換に伴うメタ情報伝播の安全性は考慮されていなかった．

本論文では，動的情報フロー制御系間でのセキュリティラベル交換に伴うメタ情報伝播を安全にするための，セキュリティラベルの仮名化手法を提案する．本手法では，Denningの示した情報フローモデル FM[1)] に基づきセキュリティラベルを複数のセキュリティラベルへと分解し，他の情報フロー制御系に開示したくないメタ情報を伴うセキュリティラベルを仮名化した上で，再度それらのセキュリティラベルを集成した複合仮名化ラベルを新たに定義する．この仮名化により他の情報フロー制御系へと開示されるメタ情報を必要最小限に抑制し，安全な動的情報フロー制御系の連係を実現する．さらに，この仮名化は副次的効果として，セキュリティラベルの改竄検知を実現し，セキュリティラベル改竄による情報漏洩を防止する．

2. セキュリティラベルの仮名化手法

2.1 概　　略

本手法が依拠するのは，セキュリティラベルは，セキュリティクラス結合という内部構造

を持つという考えである．情報フロー制御の分野では，セキュリティ分類子として，セキュリティクラスを定義し，それらの間に結合演算とフロー関係を定義する[1)]．よって，セキュリティラベルは 1 個以上のセキュリティクラス結合という内部構造を持つと見なせる．このセキュリティクラス結合という内部構造を介して，セキュリティラベルを複数のセキュリティラベルへと分解できる．

本手法では，セキュリティラベルが含むメタ情報の開示を個別に制御するために，複合仮名化ラベルを用いる．複合仮名化ラベルとは，セキュリティラベルを複数のセキュリティラベルへと，セキュリティクラス結合を介して分解し，それらのセキュリティラベルのうち，開示したくないメタ情報を伴うものを仮名化し，最後にそれらのセキュリティラベルを集成したものである．

なお，本論文では，仮名化という用語を以下の意味で用いる．すなわち，仮名化とは，ある識別子を別の識別子で代替することである．かつ，識別子と代替の識別子の対応関係は，仮名化を行った情報フロー制御系以外には公開されない．

セキュリティラベルの仮名化によって他の情報フロー制御系は本来のセキュリティラベルを認識できなくなるので，本来のセキュリティラベルに関連するメタ情報も認識できなくなる．その結果として，セキュリティラベルを選択的に仮名化した複合仮名化ラベルを介して，伝播するメタ情報を制御できる．

2.2 記　　法

記述の明確化のため，本論文の以降の部分では，下記の記法を用いる．

セキュリティラベルとセキュリティクラス

セキュリティラベルは，L を前置したアルファベットで表記し，セキュリティクラスはアルファベットで表記する．

なお，読解の容易化のため，便宜上，アルファベットは表 1 のように使い分ける．すなわち，もともと情報に付与されているセキュリティラベルを LA, LB, LC で表記する．そのセキュリティラベルを構成するセキュリティクラスのうち，他系に開示するものを I, J, K で，他系に開示しないものを P, Q, R で表記する．仮名化したセキュリティラベルのうち，本来のセキュリティラベルを (読者に) 暗示するものは LA', LB', LC' で，それ以外は LX, LY, LZ で表記する．また，後述する仮セキュリティクラスは X, Y, Z で表記する．

セキュリティクラス結合

$\oplus$ で表記する．例: $I \oplus P$

表 1　アルファベットの使い分け
Table 1　Usage of alphabetical symbols

	オリジナル	開示する	開示しない	仮名化
セキュリティラベル	LA, LB, LC	LI, LJ, LK		LA', LB', LC' LX, LY, LZ
セキュリティクラス		I, J, K	P, Q, R	X, Y, Z(仮セキュリティクラス)

フロー関係

$\rightarrow$ で表記する．例: $I \rightarrow J$

セキュリティラベルとセキュリティクラスの関係

$::=$ で表記する．例: $LA ::= I \oplus P \oplus X$

この例では，セキュリティラベル LA が内部構造として，セキュリティクラス I, P, X の結合を持つ．もしくは，セキュリティラベル LA は，$I \oplus P \oplus X$ に付けられた名前であると見なすこともできる．なお，特に断りが無い限り，あるセキュリティクラスに L を前置したものを，そのセキュリティクラスに対応するセキュリティラベルとする．例えば，$LI ::= I$.

複合仮名化ラベル

($\{$ 仮名化ラベル集合 $\}, \{$ 開示ラベル集合 $\}$) で表記する．例: $(\{LA', LX, LY\}, \{LI, LJ, LK\})$

なお，複合仮名化ラベルの詳細は 2.4 にて示す．

2.3 情報フロー制御とセキュリティラベルの仮名化

本手法の基本アイディアである，情報フロー制御の特性に基づくセキュリティラベルの仮名化について説明する．

情報フロー制御においてセキュリティクラスは基本概念の一つであり，下記の特性を持つ[1)]．

$$I \rightarrow J \wedge P \rightarrow J \Rightarrow I \oplus P \rightarrow J \quad (1)$$

この特性は,「セキュリティクラス I に属する情報は，セキュリティクラス J に属する情報へとフロー可能であり，セキュリティクラス P に属する情報も，J へとフロー可能であるならば，I に属する情報と P に属する情報から算出された情報も，J へとフロー可能である」と読める．

ここで，2 個以上の情報フロー制御系が連係する場合，ある制御系ではフロー判定結果が常に真 (フロー可能) になり，フロー判定に寄与しないセキュリティクラスが存在しうる．例えば，ある情報フロー制御系において，全ての情報がセキュリティクラス P に属し，かつ常に $\forall J \quad P \rightarrow J$ が成立するならば，その系においては，式 (1) の左辺第二項が常に真とな

るので，セキュリティクラス P はフロー判定に寄与しない．

このような，ある系においてフロー判定結果が常に真であるセキュリティクラスは，同様にフロー判定結果が常に真である仮のセキュリティクラス (以降では仮セキュリティクラスと呼ぶ) へと置換してもフロー判定結果は不変という性質を持つので，この性質を利用してセキュリティラベルを仮名化できる．すなわち，もし，ある他系に対して開示したくないメタ情報が存在し，かつ，そのメタ情報に対応するセキュリティクラスが，その他系においてフロー判定に寄与しないならば，その他系に対して該セキュリティクラスに対応するセキュリティラベルを仮名化して，メタ情報の開示を抑制でき，かつ自系とその他系は連係動作できる．

仮セキュリティクラスへの置換に基づいた，セキュリティラベルの仮名化の基本アイディアを示す (**図 1**)．図 1 の例では，P は他系においてフロー判定に寄与しないものとする．セキュリティクラス仮名化により，P が X へと置換され，セキュリティクラス P が他系に対し開示されなくなるので，P に関連するメタ情報の開示も抑制される．また，P を X に置換しても，他系におけるフロー判定結果は従来どおりであり，他系においては正常に情報フロー制御を行える．

なお，図 1 に示した基本アイディアでは，送信側でのみ仮名化が行われており，送信側と受信側と非対称であるが，本論文の以降で示す複合仮名化ラベルでは，対称になるよう構成される．つまり，連係する動的情報フロー制御系は相互に仮名化を行えるよう構成される．

また，複合仮名化ラベルでは，副次的機能としてセキュリティラベルの改竄検知も加わる．セキュリティラベルの改竄とは，セキュリティラベルを構成する一部のセキュリティクラスを置換もしくは削除することである．改竄されたセキュリティラベルを伴う情報を受信すると，適切な情報フロー制御を実施できず，情報漏洩を生じる危険性がある．セキュリティラベルの改竄検知により，このような情報漏洩を防止できる．

2.4 複合仮名化ラベル

複合仮名化ラベルは，2.3 章で示した仮名化ラベルを，送信側と受信側が対象になるように改良し，ラベル改竄検知機能を付加したものである (**図 2**)．複合仮名化ラベルは，仮名化ラベル集合と，開示ラベル集合の対から成る．仮名化ラベルとは，メタ情報伝播の抑制のために，セキュリティラベルを仮名化したものである．開示ラベルとは，他系においてフロー判定に用いるために，開示するセキュリティラベルである．仮名化ラベル集合と開示ラベル集合は，本来のセキュリティラベルをセキュリティクラス結合に分解したうえで，各セキュリティクラスをセキュリティラベルへと変換し，メタ情報伝播を抑制するために一部の

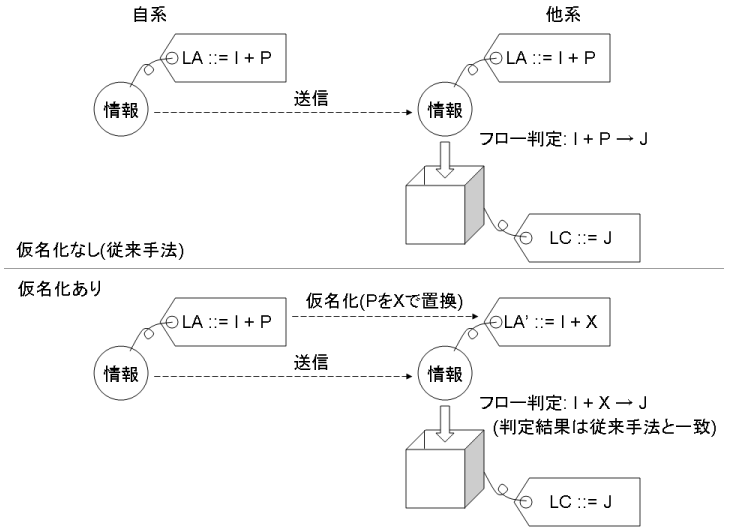

図 1 仮セキュリティクラス置換に基づいたセキュリティラベルの仮名化
Fig. 1 Security-label pseudonimization by substituting pseudo security class

セキュリティラベルを仮名化し，最後に各セキュリティラベルを集成して作成する．

複合仮名化ラベルは，下記の 3 点の特性を持つよう構成される．

- セキュリティラベルを複合仮名化ラベルへと仮名化することにより，他系においてフロー判定に寄与しないセキュリティクラスの開示を抑制し，そのセキュリティクラスに関するメタ情報伝播を抑制できる．
- 複合仮名化ラベルの受信時に仮名化を解除して，セキュリティクラス結合に仮セキュリティクラスを含むセキュリティラベルへと変換でき，そのセキュリティラベルに基づいて情報フロー制御できる．
- 複合仮名化ラベルの仮名化解除の際に，セキュリティラベルの改竄を検知できる．

2.5 複合仮名化ラベルの詳細

本章では，セキュリティラベルから複合仮名化ラベルへの変換と，複合仮名化ラベルからセキュリティラベルへの変換，そして改竄検知について例を挙げて詳細に説明する．例としては，セキュリティラベル $LA ::= X \oplus I \oplus J \oplus P$ を付与された情報を，情報フロー制御系 s1 が s2 へと送信し，処理結果として複合仮名化ラベル $(\{LA', LX, LY\}, \{LI, LJ, LK\})$ を

Vol.2009-CSEC-46 No.36
2009/7/3

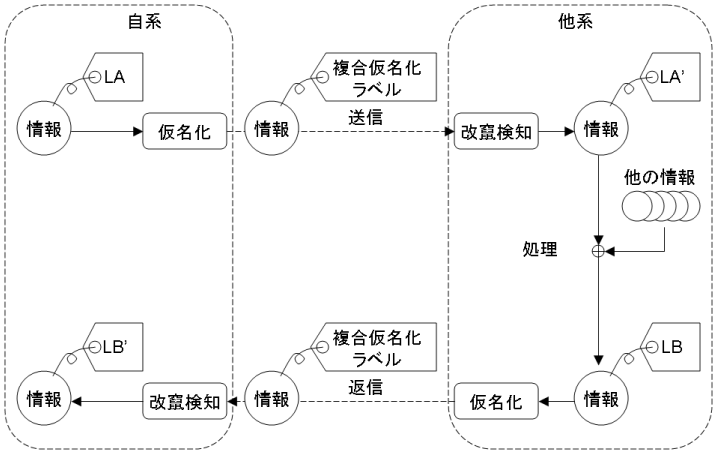

図 2 複合仮名化ラベルの基本シーケンス
Fig. 2 Interaction sequence with pseudonymized labels

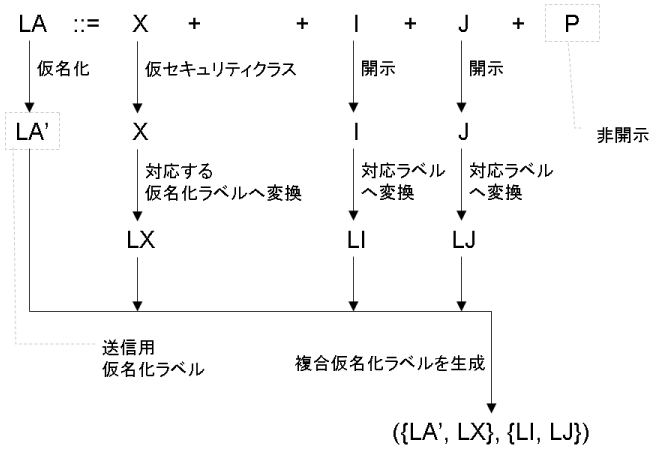

図 3 セキュリティラベルから複合仮名化ラベルへの変換
Fig. 3 Convert from security label to pseudonymized label

表 2 変換例
Table 2 Pseudonymization examples

	セキュリティラベル	変換方向	複合仮名化ラベル
送信時	$LA ::= X \oplus I \oplus J \oplus P$	$\Longrightarrow$	$(\{LA', LX\}, \{LI, LJ\})$
受信時	$LB' ::= X \oplus Y \oplus I \oplus J \oplus K \oplus P$	$\Longleftarrow$	$(\{LA', LX, LY\}, \{LI, LJ, LK\})$

付与された情報を，s1 が s2 から受信する場合を取り上げる (表 2).

2.5.1 セキュリティラベルから複合仮名化ラベルへの変換手順

セキュリティラベルから複合仮名化ラベルへの変換手準 (仮名化手順) を示す (**図 3**).

仮名化手順の第一の特徴は，複数の仮名化ラベルからなる仮名化ラベル集合を用いる点である．これは送信側と受信側の手順を対称にするためである．

仮名化手順の第二の特徴は，P に対応するセキュリティラベルを仮名化する代わりに，本来のセキュリティラベル LA を仮名化する点である．これは改竄検知機能を複合仮名化ラベルに付与するためである．

後に情報が返信される時に備えて，送信元システム s1 は 3 項組 $\langle s2, LA, LA' \rangle$ を記憶する．ここで s2 は送信先システムの識別子である．この 3 項組を参照して，s2 から s1 への情報返信時に，s1 において複合仮名化ラベルをセキュリティラベルへと変換する．この変換処理については 2.5.2 で説明する．

2.5.2 複合仮名化ラベルからセキュリティラベルへの変換手順

複合仮名化ラベルからセキュリティラベルへの変換手順 (仮名化解除手順) を示す (**図 4**).

仮名化解除手順の特徴は，仮名化ラベル集合のうち，自系が過去に生成した仮名化ラベル (LA') と，他系が生成した仮名化ラベル (LX, LY) を区別して扱う点である．自系が過去に生成した仮名化ラベルは，記憶しておいた 3 項組み $(\langle s2, LA, LA' \rangle)$ に基づいて仮名化を解除する．他系が生成した仮名化ラベルには，仮セキュリティクラスを適宜割り当てる．

仮名化解除結果 LB' が s1 上に定義されていない場合，つまり $X \oplus Y \oplus I \oplus J \oplus K \oplus P$ と構成されるセキュリティラベルが存在しない場合，s1 は新規に LB' を割り当てる．既に適切な LB' が存在するならば，それを再利用する．

なお，LK のような他系からの開示ラベルに対応するセキュリティクラスを，s1 が知らない場合 (つまり未知のセキュリティラベルを開示された場合)，未知の開示ラベルを含む

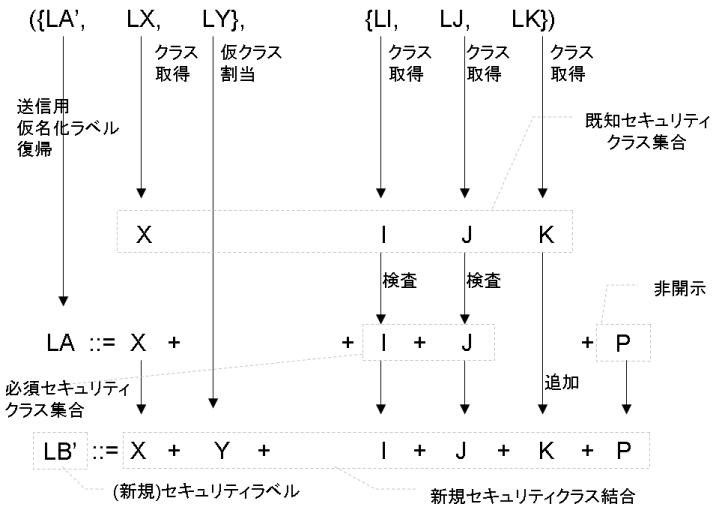

図 4 複合仮名化ラベルからセキュリティラベルへの変換
Fig. 4 Convert from pseudonymized label to security label

複合仮名化ラベルが付与された情報を，s1 はセキュリティ違反として破棄する．なぜならば，その情報について s1 上で適切なフロー判定を行えないからである．つまり，開示するセキュリティクラスと，そのセキュリティラベルの対応については，複合仮名化ラベルの変換アルゴリズムとは別に，事前に s1 と s2 の間で情報交換 (事前設定) しておく必要がある．

2.5.3 複合仮名化ラベルの改竄検知手順

s1 は複合仮名化ラベルの受信時に，2.5.2 に示す変換とともに，複合仮名化ラベルの改竄を検知するための検証を行い，情報漏洩を防止する．改竄によって，複合仮名化ラベルを構成する開示ラベルの一部を置換もしくは削除された場合，仮名化解除したセキュリティラベルを構成するセキュリティクラス結合の一部が置換もしくは欠落するので，情報フロー制御が異常動作して情報漏洩する危険性がある．改竄検知によって，そのような情報漏洩を防止できる．

改竄検知の手順は次の通りである．まず，LA' を記憶しておいた 3 項組みに基づいて仮名化解除し，以前の送信時に開示したセキュリティクラス群 (I, J) を算出し，必須セキュリティクラス集合とする．次に，複合仮名化ラベル $(\{LA', LX, LY\}, \{LI, LJ, LK\})$ を構成するセキュリティラベルから，自系が生成した仮名化ラベル (LA') と，未知の (今回新規に受信した) 仮名化ラベル (この例では LY) を取り除き，残ったセキュリティラベル群に対応するセキュリティクラス群 (LY, LI, LJ, LK) を，既知セキュリティクラス集合とする．そして必須セキュリティクラス集合が既知セキュリティクラス集合に包含されることを検査し，この検査に合格しない複合仮名化ラベルを伴う情報は，セキュリティ違反として破棄する．この検査により，LA には含まれていたにもかかわらず，s2 が s1 へと返信した情報の複合仮名化ラベルでは欠落しているセキュリティクラスがあれば検知できる．

3. 結　　果

セキュリティラベルを介したメタ情報の漏洩を，2 章で示した手法によりどのように防止するかを，2 個の事例を想定して説明する．想定事例 1 では，セキュリティラベルが不当に照合される事態を想定し，複合仮名化ラベルの利用によって，セキュリティラベルの照合によるメタ情報の漏洩を防止できることを確認する．想定事例 2 では，セキュリティラベルが改竄される事態を想定し，複合仮名化ラベルの利用によって，セキュリティラベルの改竄を検知でき，改竄によるメタ情報の漏洩を防止できることを確認する．

3.1 想定事例 1: セキュリティラベル照合を介したメタ情報漏洩の防止

複合仮名化ラベルの利用により，情報フロー制御系が連係する際に，セキュリティラベルの照合による情報漏洩を防止できる．まず，セキュリティラベルの照合による情報漏洩について説明する．次に，複合仮名化ラベルの利用による情報漏洩防止の仕組みについて説明する．

セキュリティラベルの照合による情報漏洩とは，複数のセキュリティラベルを不当に照合されることにより，セキュリティラベルの持つメタ情報が漏洩することを指す．より詳細には，複数のセキュリティラベルについて，それらを構成するセキュリティクラス結合が照合されることにより，セキュリティラベルの含むメタ情報が漏洩することを指す．

セキュリティラベルの照合による情報漏洩について，オンラインショップにおけるユーザの購入動向情報が漏洩する例を示す (**図 5**)．あるユーザ P が，オンラインショップ I と J に対して，それぞれ発注 1 と発注 2 を行い，各オンラインショップがショップ毎に会計を行う会計サービスに対して，会計依頼 i と j を行う．ここで，ユーザ P に関する情報であることをセキュリティクラス P で示し，ショップ I および J に関する情報であることをセキュリティクラス I および J で示すと，発注 1 および 2 のセキュリティラベルは $LA1 ::= P, LA2 ::= P$ となり，会計依頼 i および j のセキュリティラベルは $LBi ::= I \oplus P, LBj ::= J \oplus P$ とな

Vol.2009-CSEC-46 No.36
2009/7/3

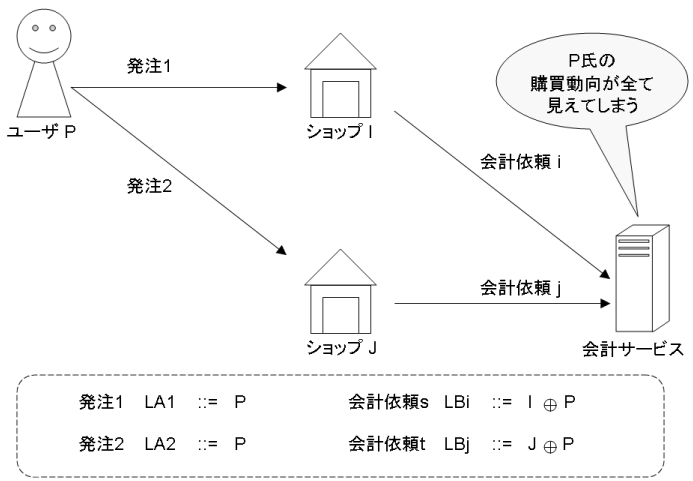

図 5 セキュリティラベル照合によるメタ情報漏洩
Fig. 5 Meta-information leak by cross checking security-labels

る．ここで，会計サービスにおいては，LBi と LBj の両方に含まれるセキュリティクラス P を照合できるので，ユーザ P のオンラインショップ I と J にまたがる購入動向が会計サービスへと情報漏洩する．

上記のオンラインショップの例において，複合仮名化ラベルの利用により，購入動向の情報漏洩を防止できる．オンラインショップ I を制御する情報フロー制御系 si が，会計依頼 i のセキュリティラベルを複合仮名化ラベル ($\{LBi'\}\{LI\}$) へと変換し，オンラインショップ J を制御する情報フロー制御系 sj が，会計依頼 j のセキュリティラベルを複合仮名化ラベル ($\{LBj'\}\{LJ\}$) へと変換する．その結果，会計サービスにおいては，ユーザ P の購入動向を把握できなくなり，購入動向の情報漏洩を防止できる．なぜならば，LBi' と LBj' が，ユーザ P のセキュリティクラス P を含むことを，会計サービスは知らないためである．この際に，LI と LJ は開示されているので，依然として会計サービスにおいて，オンラインショップ I とオンラインショップ J からの会計依頼を混同しないように情報フロー制御できる．

3.2 想定事例 2: セキュリティラベル改竄を介した情報漏洩の防止

複合仮名化ラベルの利用により，情報フロー制御系が連係する際に，セキュリティラベルの改竄による情報漏洩を防止できる．まず，セキュリティラベルの改竄による情報漏洩について説明する．次に，複合仮名化ラベルの利用による情報漏洩防止の仕組みについて説明する．

セキュリティラベルの改竄による情報漏洩とは，送信した情報が処理後に返信される際に，返信情報のセキュリティラベル，もしくはそれを仮名化した複合仮名化ラベルが改竄されることにより，情報が漏洩することを指す．ここでいう情報はメタ情報ではなく，セキュリティラベルが付与された情報そのものである．

セキュリティラベルの改竄による情報漏洩について，CRM サービスにおいてユーザの購入履歴情報が漏洩する例を示す (**図 6**)．あるユーザ I が，オンラインショップ J に対して発注 i を行い，オンラインショップ K が CRM サービスに対して，発注記録 i の管理を依頼する．そして，ユーザ I は自身の発注記録を閲覧 i により閲覧する．ここで，ユーザ I，後述するユーザ J，オンラインショップ K に関する情報であることを，それぞれセキュリティクラス I, J, K で示すと，発注記録 i のセキュリティラベルは $LBi ::= I \oplus K$ となるので，I 氏の発注履歴のセキュリティラベルも $LCi ::= I \oplus K$ となる．ここで CRM サービスが I 氏の発注履歴のセキュリティラベルを $LCi ::= J \oplus K$ と改竄 (I を J で置換) すると，オンラインショップ K の情報フロー制御系 sk は，誤ってユーザ J へと I 氏の発注履歴を開示してしまい，I 氏の発注履歴が情報漏洩する．また，CRM サービスが I 氏の発注履歴のセキュリティラベルを $LCi ::= K$ と改竄 (I を削除) すると，オンラインショップ K の情報フロー制御系 sk は，誤って公開ネットワークへと I 氏の発注履歴を開示してしまい，I 氏の発注履歴が情報漏洩する．

上記の CRM サービスの例において，複合仮名化ラベルの利用により，発注履歴の情報漏洩を防止できる．オンラインショップ J を制御する情報フロー制御系 sk が，発注記録 i のセキュリティラベルを複合仮名化ラベル ($\{LBi'\}\{LI, LK\}$) へと変換する．すると，I 氏の発注履歴の複合仮名化ラベルも同様に $\{LBi'\}\{LI, LK\}$) となる．その結果，CRM サービスによるセキュリティラベルの改竄を検知でき，発注履歴の情報漏洩を防止できる．なぜならば，LBi' が I を含み J を含まないことを情報フロー制御系 sk は 3 項組 $\langle sc, LEi, LEi' \rangle$(sc は CRM サービスの情報フロー制御系) によって記憶しているため，sk での仮名化解除において I の置換や欠落を検知できるからである．なお，CRM サービスが事前にユーザ J の発注記録 j(複合仮名化ラベル ($\{LBj'\}\{LJ, LK\}$)) を受信していた場合，ユーザ I の発注履歴

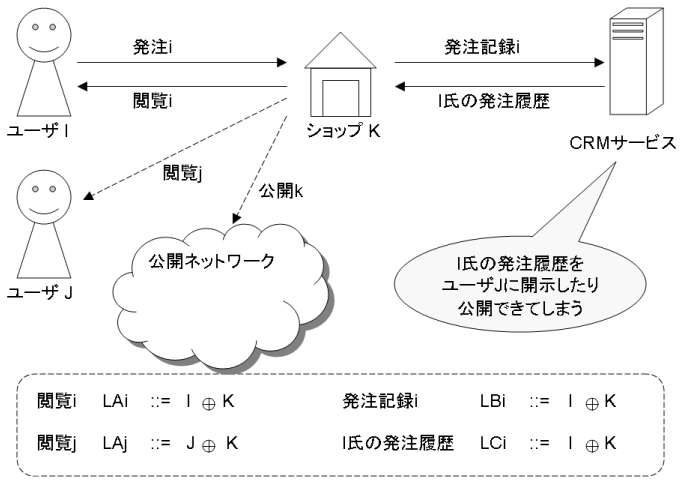

図 6 セキュリティラベル改竄による情報漏洩
Fig. 6 Information leak by falsificating security-label

の複合仮名化ラベルを $(\{LBj'\}\{LJ, LK\})$ へと改竄することにより，ユーザ J へと情報を漏洩させうる．ただし，CRM サービスがこの改竄を行うには，LJ と必ず同時に出現する仮名化ラベル LBj' を事前の分析により突き止めておく必要がある．そのため，複合仮名化ラベルを用いない場合より，改竄は難しくなっている．

4. 関 連 研 究

情報フロー制御の理論的基礎は Denning が示した情報フローモデル FM である[1]．このモデルはセキュリティクラス，セキュリティクラス結合，フロー関係などの概念を含む．筆者等の手法も，このモデルに基づいている．

セキュリティラベルを介した情報の伝播を制御できるセキュリティラベルのモデルの一つに，Myers らが示した Decentralized Label Model がある[3]．このモデルでは，セキュリティラベルをプログラムにおいて第一級 (first class) の要素として扱え，この第一級ラベルにたいしてセキュリティラベルを付与でき，結果としてセキュリティラベルを介した情報の伝播を制御できる．また，このモデルでは，セキュリティラベル間の代行関係を定義でき，個別に安全性を検証した複数のプログラムの，連係動作の安全性を検証できる．しかし，セキュリティラベルは一括して開示制御され，メタ情報の一部を開示することはできない．また，情報フロー制御系の個数は示されておらず，他系との連係動作は示されていない．

動的な情報フロー制御系の一つに，吉濱らが示した動的アプローチによる言語ベースの情報フロー制御がある[2]．このアプローチでは，情報にセキュリティラベルを付与し，実行時にフロー判定を行える．また，情報フロー制御系の外部に，セキュリティラベルを付与したデータを保存できるデータベース管理システムを接続できる．しかし，このデータベースに格納する情報のセキュリティラベルが含む，メタ情報の伝播制御については示されていない．

複数の情報フロー制御系の連係動作において，全体の情報フローを制御する手法を，大田らが示している[4]．この手法では，各系内での情報フロー制御を有向グラフとしてモデル化し，それらを連結したグラフを分析して，危険な情報フローを生じる経路を探索し，危険な経路がある場合には，グラフの枝の一部を削除するよう，情報フロー制御を変更することで，全体の情報フローを制御する．しかし，セキュリティラベルを介したメタ情報の伝播については言及されていない．

携帯電話の契約者固有 ID 利用に伴うプライバシー問題を，楠，高木らが指摘している[5),6)]．これらは，ユーザに関連付けられた ID を，携帯電話が複数のサイトへと開示することにより，ユーザのプライバシー侵害が生じる危険性を指摘したものである．筆者等の研究は，動的情報フロー制御系の連係における，同様の危険性を解消するものである．

5. 考　　察

5.1 情報フロー制御系の相互信頼と仮名化

情報フロー制御系が相互に信頼していても，セキュリティラベルの仮名化には意味があると筆者等は考えている．まず，複数の情報フロー制御系が連係する場合，相互に信頼関係が成立する必要がある．なぜならば，他系でセキュリティラベルに従った情報フロー制御が正しく行われることが，連係の前提となるからである．ここで，他系を信頼しているならば，セキュリティラベルを仮名化する必要性は無いという考えもあろう．しかし，他系を無限に信頼することは現実的ではなく，他系が攻撃者に侵入されたり，他系との間の通信経路で攻撃を受ける可能性を考慮すると，セキュリティラベルの仮名化は必要であると筆者等は考える．また，他系がいかなる攻撃にも耐えることを要求するならば，他系の情報セキュリティのコストが上昇し，コストが高すぎる場合には連係動作は実施されないので，やはりセキュリティラベルの仮名化は必要であると筆者等は考える．

5.2 仮名化ラベルの生成手法

仮名化ラベルは，複数の情報フロー制御系で一意となるよう生成しなければならない．例えば，LA を LA' へと仮名化する場合，LA' は連係する情報フロー制御系全体で一意でなければならない．もし，自系で生成した仮名化ラベルと，他系で生成した仮名化ラベルが衝突すると，正しく仮名化解除を行えない．よって，複数の動的情報フロー制御系が，それぞれ仮名化ラベルを生成しても，衝突が起きないような生成手法が必要である．そのような LA' の生成手法として例えば UUID[7] が挙げられるが，UUID は生成時刻に関する情報を持つので，仮名化へ応用するには安全性の検討が必要である．

5.3 フロー判定に寄与するセキュリティクラスのメタ情報開示制御

本論文で示した手法では，開示したくないメタ情報に対応するセキュリティクラスが，他系においてフロー判定に用いられている場合には，メタ情報を秘匿できない．これは本手法が，フロー判定が常に真であるセキュリティクラスの，仮セキュリティクラスへの置換に基づいているためである．しかしながら，常に真という条件を緩和し，自系と他系でフロー判定は一致しつつ，識別子としての対応関係は秘匿できるような，新たな仮セキュリティクラスを定義することで，フロー判定に寄与するセキュリティクラスのメタ情報開示も制御できる可能性がある．

5.4 セキュリティラベル改竄検知の制限事項

本論文で示した手法では，3.2 章の末尾で示したように，仮名化ラベル集合と，開示ラベル集合を同時に改竄された場合に，改竄検知できないという制限がある．仮名化ラベルと開示ラベルの関係は，仮名化を実施した系以外には明示されないとはいえ，仮名化ラベルと開示ラベルの共起関係を別途調査することで，上記の同時改竄攻撃が可能となる．仮名化ラベルと開示ラベルの共起関係は，長期にわたる複数の複合仮名化ラベルの観察により推測可能である．この同時改竄攻撃への対処としては，仮名化ラベルを一定期間で変えることが考えられる．例えば，あるセキュリティラベル LA の仮名化ラベルを，日毎に $LA'_0, LA'_1, ...$ と変える．これにより，仮名化ラベルと開示ラベルの共起関係の推測を困難にできる．しかしながら，この対処によっても同時改竄攻撃を完全には防止できない点に注意が必要である．

6. 結　　論

情報フロー制御系の連係動作においては，セキュリティラベルを介したメタ情報漏洩の危険性がある．筆者等はこのメタ情報漏洩を防止するため，セキュリティラベルを仮名化する手法を示した．この手法はセキュリティラベルをセキュリティクラス結合を介して複数のセキュリティラベルへと分解し，それらのセキュリティラベルについて個別に開示と仮名化を制御する．この仮名化により，セキュリティラベルの照合によるメタ情報の漏洩とセキュリティラベルの改竄による情報漏洩を防止できることを，それぞれ事例を想定して示した．今後の課題としては，複数の情報フロー制御系で一意かつ安全な仮名化ラベルの生成手法の決定，フロー判定に寄与するセキュリティクラスのメタ情報開示制御方の開発，セキュリティラベル改竄検知の制限事項への対処が挙げられる．

参 考 文 献

1) Dorothy E. Denning: A Lattice Model of Secure Information Flow, *Communications of the ACM*, Vol.19, No.5, p.236.
2) 吉濱佐知子，工藤道治，小柳和子：動的アプローチによる言語ベースの情報フロー制御，情報処理学会誌， Vol.48, No.9, p.3060.
3) Andrew C. Myers and Barbara Liskov: A Decentralized Model for Information Flow Control, *Proceedings of the sixteenth ACM symposium on Operating systems principles*, p.129.
4) 大田幸由，由比藤光宏，　萱野忠：連合システムにおける情報フロー制御に関する一考察，電子情報通信学会ソサイエティ大会講演論文集，p.125 (1995).
5)　楠正憲：携帯 ID 開放の危うさ・事件が起きる前に対策を，http://it.nikkei.co.jp/internet/news/index.aspx?n=MMITbf000029092008 (2008).
6) 高木浩光：契約者固有 ID とは，http://itpro.nikkeibp.co.jp/article/Keyword/20081007/316269/ (2008).
7) P. Leach, M. Mealling and R. Salz: A Universally Unique IDentifier (UUID) URN Namespace (2005). (RFC 4122).