DEWS2006 3C-i8

# トレーサビリティにおいて追跡対象者の構成を秘匿しながら検証可能にする手法

小金山美賀† 渡邊 裕治† 百合山まどか† 吉澤 武朗†

† 日本アイ・ビー・エム（株） 東京基礎研究所
E-mail: †{mkogane,muew,yuriyama,ytakeo}@jp.ibm.com

**あらまし** トレーサビリティとは，商品，製品やその部品の，処理や流通経路などの履歴を追跡可能にする技術である．トレーサビリティを適用することにより，追跡対象となるものを提供するサプライヤーの情報やサプライヤー間の関連を追跡することができる．一方で，情報の検証可能性を高めるということは，サプライヤーの詳細情報や取引関係など，ビジネス上秘匿しておきたい情報を公開しなければならないことを意味する．逆に情報の秘匿を優先し，すべての情報を非公開にすれば，検証可能性が失われトレーサビリティとして機能しなくなってしまう．そこで，秘匿したい情報は非公開にしたまま，トレーサビリティに必要な検証可能性を実現する手法を提案する．本稿では，あらかじめ登録されたグループメンバが署名したことは検証できるが，メンバ個人を特定することはできないというグループ署名の技術を利用して，秘匿したい情報を非公開にしたまま，必要な検証可能性を実現する手法について述べる．
**キーワード** プライバシー保護，トレーサビリティ，グループ署名，情報統合，情報検索

# A Method for Verifiable and Anonymous Traceability Flow

Mika KOGANEYAMA†, Yuji WATANABE†, Madoka YURIYAMA†, and Takeo YOSHIZAWA†

† IBM Research, Tokyo Research Laboratory, IBM Japan, Ltd.
E-mail: †{mkogane,muew,yuriyama,ytakeo}@jp.ibm.com

**Abstract** Traceability is the ability to trace the process history and the distribution channels of products and their parts. We can trace the information about target suppliers and the relationship between them by using traceability. Meanwhile, to increase verifiability of traceability flow means that target suppliers have to disclose confidential business information and relation. Reversely, keeping all information private to give priority to protect confidentiality, the verifiablilty is lost and traceability doesn't work. We propose a method to satisfy the necessary verifiability and suppliers' anonymity for traceability. In this paper, we realize the method by group signature which has properties that the receiver of the signature can verify that it is a valid signature of a group, but cannot discover which member of the group made it.
**Key words** Privacy Protection, Traceability, Group Signature, Information Integration, Information Retrieval

## 1. はじめに

### 1.1 トレーサビリティと秘匿情報

近年，自動車のリコールや商品偽造などの問題が取りざたされていることから，消費者に対して製品の安全性や信頼性を示すための技術としてトレーサビリティが注目されている．トレーサビリティとは，商品，製品やその部品の，処理や流通経路などの履歴を追跡可能にする技術である．例えば，ある製品が複数の部品を組み合わせることにより製造されるとき，トレーサビリティによって，その製品の部品がどこで提供されたのか，どのような処理を経て製品が製造されたのかを追跡することができる．

一方，トレーサビリティが実現されることによって，追跡対象者である製品や部品の提供者，処理者，流通者などのオブジェクトサプライヤー（以下サプライヤーと表記する）が本来知られたくない情報までもが，追跡過程において知られてしまう可能性がある．例えば，自動車の部品を提供する部品工場や，組立工場，ディーラーなどからなるサプライチェーンにおける，自動車部品のトレーサビリティについて考える．トレーサビリティによって，自動車のある部品に故障があった際に，どの工場から仕入れた部品であるか，その工場で製造された部品を使っている自動車の車体番号は何番か，などを追跡することができる．またディーラーは，自動車の製造過程を追跡することにより，契約している工場が，あらかじめ提示した製品品質レ

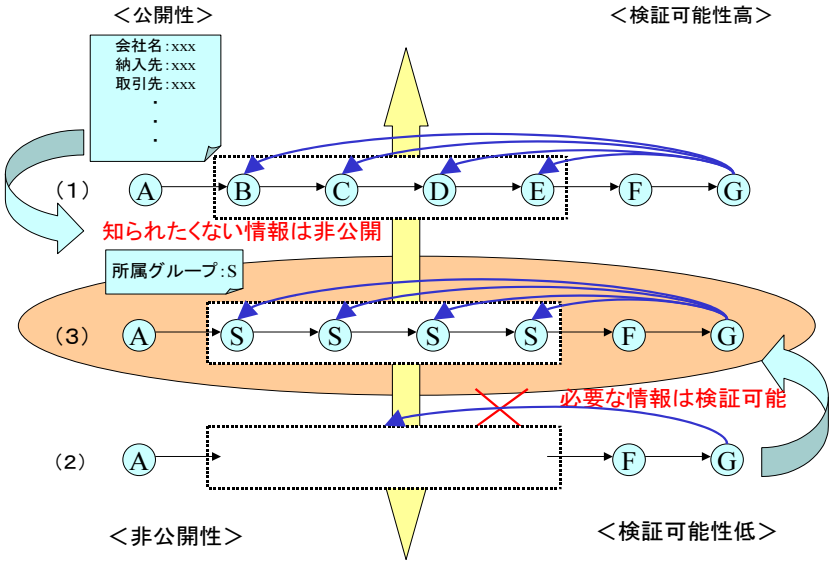


図 1　公開性と検証可能性の関係

ベルの取引工場から部品の仕入れや組立を行っているかどうかを検証することができる．しかし同時に，ディーラーと契約している工場は，自分の取引工場の具体的な名前や詳細情報，取引関係など，知られたくない情報までディーラーに知られてしまう可能性がある．取引状況や取引先情報を第三者に知られることは，ビジネス上において大きな不利益をもたらす可能性がある．

そこで本稿では，サプライヤーが非公開にしたい情報は秘匿しながら，トレーサビリティで必要な検証可能性を実現する手法について提案する．

### 1.2　課　　題

図 1 は，トレーサビリティにおける公開性と検証可能性の関係を示した図である．A から G はサプライヤー，サプライヤー間の矢印は処理フローの流れ，すなわち取引関係を表している．破線で囲まれたフローは，サプライヤー F が非公開にしたいサプライヤー情報や取引関係である．このとき G が追跡者で，A から F までのフローを検証したいとする．

図 1 の (1) は，サプライヤー間の検証可能性を高める一方で，本来非公開にしたい情報もすべて公開する必要があることを示している．これは，非公開にしたい情報の秘匿を考慮しないトレーサビリティの場合に当てはまる関係である．図 1 の (2) は，情報の秘匿を優先し，すべての情報を非公開にするため，検証可能性が低くなることを示している．この場合，追跡者自身は破線で囲まれたフローの情報をまったく知ることができず，その情報を知る特定の者に，追跡結果を問い合わせることしかできなくなってしまう．

本稿で対象としている課題は，図 1 の (1) と (2) で実現している公開性と検証可能性のそれぞれ中間に位置する，図 1 の (3) に示すような考え方を実現することである．図 1 の (3) は，破線で囲まれたフローに存在するサプライヤーの具体的な名前などを特定することはできないが，S という品質レベルで分類されたグループに所属し，4 つのサプライヤーが関連していることを検証できることを示している．つまり，具体的な名前や関係など，サプライヤーが知られたくない情報は非公開にしたまま，追跡者が承認する品質レベルのオブジェクトを提供するサプライヤーであるか，サプライヤー間のフローが正当なものであるかといった必要な検証可能性を満たすことになる．

さらに，オブジェクトの品質に問題が生じたなど，何らかのトラブルが発生した場合は，非公開性を解除できる存在，すなわち非公開解除可能性の実現が必要である．サプライチェーン間のいずれかにトラブルが発生した場合は，非公開性を解除する，つまりサプライヤーの非公開情報の特定や，非公開にしていたサプライヤー間の具体的な関係を明らかにして追跡するにより，原因を調査する．

以上のことをまとめると，一般的なトレーサビリティにおける追跡対象者の関係を，

- オブジェクトの流れが，サプライヤー A → B → … → F → G の順であるトレーサビリティがあるとする．
- F と G は直接取引し，B～E は F の取引サプライヤーで，G に対して自身の詳細情報は非公開である．
- G は F から受け取るオブジェクトが初めに A を経ていることを知っている．
- G は A～E 間で流れるオブジェクトを追跡する．

と考えるとき，以下に定義する検証可能性，非公開性，非公開解除可能性を同時に満たすトレーサビリティを実現する必要がある．

**【検証可能性】**

- F の取引サプライヤーは，G が承認している品質レベルのオブジェクトを提供するサプライヤーである．
- サプライヤー間のフローが正当なものである．

**【非公開性】**

- F の取引サプライヤーは B～E である．
- サプライヤー間の具体的なフローは，B → C → D → E である．

**【非公開解除可能性】**

- 権限をもつ第三者のみが，非公開性であげた項目を検証可能にすることができる．

上記の定義を満たすようなトレーサビリティを適用すれば，1.1 節で挙げた工場のサプライチェーンにおける自動車部品のトレーサビリティの例においても，ディーラーは，契約工場が契約時に提示した製品品質レベルの工場から，仕入れや組立を行っていることを検証することができる．つまり，ディーラーが仕入れた自動車は，正規のサプライチェーンを経て製造されていることを検証することができる．また契約工場は，取引工場の具体的な名前などの詳細情報や取引工場の関連など，非公開にしたい情報をディーラーには知られないまま，正規の取引工場を使っていることを証明することができる．また，サプライチェーン間で何らかのトラブルが発生した場合には，権限を持つ第三者が非公開の情報を特定し，トラブルとなった原因を調査することができる．

本稿では，上記の定義を満たすようなトレーサビリティを実現する手段として，グループ署名を用いた手法を提案する．

### 1.3 関 連 研 究

グループ署名を用いて，個人情報を秘匿しながら必要な要件を検証する手法を実現した事例として,「プライバシを保護する匿名認証システムの開発」があげられる [1]．この事例は，サービス提供者に個人情報を知られることなく，正当な利用者へサービスを提供する認証基盤としてグループ署名を適用している．この事例は，以下のようなシナリオに適用している．

- 被検証者であるサービス利用会員同士のつながりはない．
- 被検証者である会員自身が，自分のプライバシを保護したいと同時に，サービスを利用する権限を持つことを証明したい．
- グループメンバである利用者個人を特定できるのは，会員管理者のみである．
- 利用者個人はグループメンバであり，サービス提供者は正当な利用者かを検証する者であり，会員管理者はグループメンバを管理する者で，これらの役割が変化することはない．

一方，本稿での課題の対象となるトレーサビリティに対して実現するプロトコルは，以下のようなシナリオに適用する必要がある．

- 被検証者であるサプライヤー同士が関連を持つ．
- 被検証者の情報を秘匿したり，被検証者が提供するオブジェクトの品質レベルを証明したいのは，被検証者自身ではなく被検証者と取引をしているサプライヤーである．
- グループメンバの管理者だけでなく，取引するサプライヤー自身もグループメンバである取引サプライヤー個人の詳細情報を知っている．
- 同じサプライヤーが，検証者，被検証者，被検証者と取引するサプライヤーであるなど，立場が状況によって変化する．

被検証者間の関連の存在有無や，検証過程における立場の変化などの点で，事例としてあげたシステムとは実現したいシナリオが異なる．そこで，本稿でのシナリオに対して適用できる新たなプロトコルを示す必要がある．

## 2. 課題解決のための要件

1.2 節で述べた課題を解決するための要件を，具体的なシナリオを用いて説明する．

### 2.1 シ ナ リ オ

具体的なシナリオとして，簡略化した自動車部品のトレーサビリティを挙げる．自動車部品トレーサビリティにおいて，以下のようなサプライヤー A〜G が存在するとする．

**サプライヤー A：** G，F の取引工場
**サプライヤー B〜E：** F の取引工場
**サプライヤー F：** A〜E の取引工場，G の契約工場
**サプライヤー G：** A，F と契約する自動車ディーラー

取引工場には，直接取引を行う場合だけではなく，部品を受け取るまでの過程で利用するために指定した工場も含まれている．例えば，サプライヤー B〜E は，すべてのサプライヤーが F と直接取引しているわけではなく，F が部品を受け取るまでの過程でサプライヤー B〜E のみで取引を行っている．

A〜F の工場や自動車ディーラーが以下のようなサプライチェーンを構成し，図 2 のようなフローとなる．

（1） A は，製造した部品を B に納入する．
（2） B は，A から受け取った部品を加工し，D に納入する．
（3） C は，製造した部品を D に納入する．
（4） D は，B と C から受け取った部品を組み合わせ，加工し，E に納入する．
（5） E は，D から受け取った部品を加工し，F に納入する．
（6） F は，G に自動車を納入する．

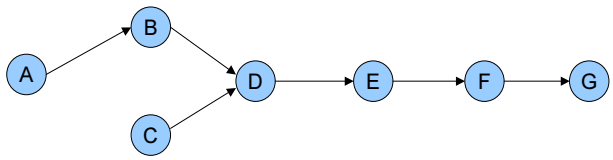


図 2　サプライチェーンの構成

また，F は G との契約時に，F の取引工場は製品品質レベル A 以上（レベル AAA〜DDD までのランク付けがあるとする）の日本の工場であることを提示している．

本シナリオでは，以下の項目を実現するトレーサビリティである必要がある．

（1） G は，F から納入した自動車が，A で製造した部品を用いて，F の提示どおりの取引工場を経て製造されたものかを検証したい．
（2） F は取引工場の詳細情報や，取引関係を G に知られたくない．
（3） サプライチェーン内で何らかのトラブルが発生した際には，工場の特定などをして，原因を調査したい．

### 2.2 解決のための要件

2.1 節のシナリオにおいて，1.2 節で述べたような検証可能性，非公開性，非公開解除性を実現するためには，それぞれ以下のような要件を満たす必要がある．

**【検証可能性】**

検証可能な項目とは，G が検証できる情報，すなわち G に対して公開してもよい情報のことである．本シナリオでは，以下の 3 つの項目が検証可能である（図 3）．

- F が納入する自動車は，A で製造された部品を用いて製造されている．
- A から部品を仕入れ，F に部品を納入するまでに 4 つの工場を経て，部品の製造や，加工，組立を行っている．
- 4 つの工場は，F の取引工場で，製品品質レベルが A 以上の日本の工場である．

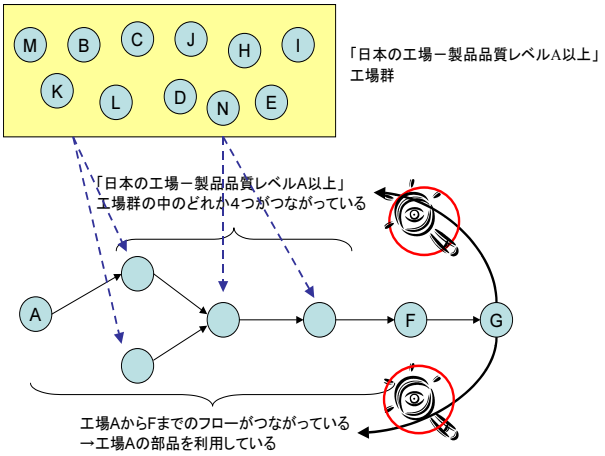


図 3　追跡可能性を満たす要件

**【非公開性】**

非公開の項目とは，G が検証することのできない情報で，G に対して公開している情報からは知ることができない．本シナリオでは，以下の 3 つの項目が非公開となる（図 4）．

- F が取引している製品品質レベル A 以上の日本の工場は，B，C，D，E である．
- A から部品を仕入れる工場は B であり，F へ部品を納入する工場は E である．
- B と C が D へ部品を納入し，D は E へ部品を納入する．

**【非公開解除可能性】**

非公開解除可能性とは，サプライチェーンの間に何らかのトラブルがあり，その原因を調査したい場合に，B～E 個々やそれぞれの納品先を特定できることである．本シナリオでは，以下のような制約条件のもとで，非公開性であげた項目が特定可能となる（図 4）．

- 特定する権限は，サプライチェーン外の第三者のみに与えられている．
- G に対する非公開性は保たれる．
- 権限を持つ第三者は，G の依頼により特定を行う．

上記の検証可能性と非公開性を同時に実現することにより，G は F が提示どおりの品質レベルの工場から正規の処理を経て部品を仕入れているかを検証することができ，製品の品質が保証される．また，F は G に対して，取引工場名や各取引工場の納品先といった詳細情報を非公開にしながら，提示どおりの工場と取引していることを証明することができる．よって通常は，これらの検証可能性と非公開性を実現することにより，G

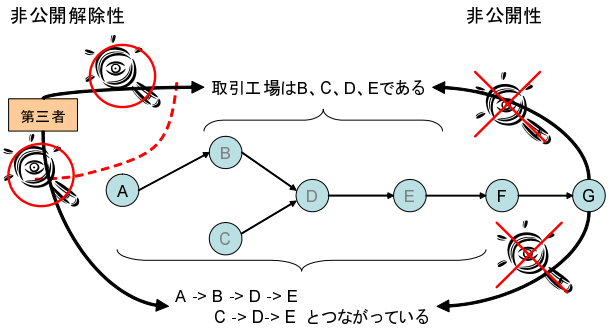


図 4　非公開性と非公開解除可能性性を満たす要件

と F は，お互いの要求を満たすことができる．

また何らかのトラブルが発生した場合には，非公開解除可能性を実現することにより，第三者が B～E の特定と検証を行うことができ，G に対する B～E の非公開性は保ったまま，トラブルの原因を調査することができる．

## 3.　準　　備

### 3.1　グループ署名

2. 章で述べた要件を実現するために，グループ署名を用いた実現方式を提案する．グループ署名は，Chaum らによって初めて提案された署名方式で，以下のような機能を実現する [2]．

（1）　グループのメンバのみが署名可能である．

（2）　グループ署名文を受け取った誰もが正当性を検証可能であるが，グループメンバの誰が署名したのかを特定することはできない．

（3）　万一の場合は，権限を持つ者によって署名者個人の特定が可能である．

以上のような機能を実現するためには，少なくとも以下の性質を持つ必要がある [3]．

**Unforeability**　署名文の偽造は行えない．

**Anonymity**　どのような署名文に関しても，あらかじめ決められた管理者以外は，署名者を特定することが困難である．

**Unlinkability**　異なる 2 つの署名文が，同一のグループメンバによって生成されたかどうかを判定することは，あらかじめ決められた管理者以外には困難である．

**Identifiability**　あらかじめ決められた管理者は，どのような署名文に対しても，いつでもその署名者を特定することができる．

**Exculpatability**　グループメンバは，自分自身が生成した署名文以外に関して責任を負わされることはない．

トレーサビリティにおいて，グループ署名の機能を利用したプロトコルを確立することにより，2.2 節で述べた要件を実現する．

### 3.2　エンティティ

2. 章で述べた要件の実現のために必要なエンティティを，3.1 節で述べたグループ署名の性質をもとに考える．

グループ署名は，署名者がグループのメンバであることは検証できるが，個人を特定することはできない性質を持つ．この

性質から，取引先を知られたくないサプライヤーは，自分の取引サプライヤーをグループメンバとして登録し，取引サプライヤーはグループ署名によってメンバであることを証明すればよい．正当なサプライヤーを経て処理，納品されているかどうかを検証したいサプライヤーは，各サプライヤーがグループ署名を行った署名文を検証することにより，正当性を自ら検証することができる．よってエンティティとして，自分の取引サプライヤーをグループ登録する者，グループメンバとなる者，グループメンバを検証する者が存在することになる．

あらかじめ決められた管理者は，署名者個人の特定が可能であるというグループ署名の性質から，詳細情報を非公開とするサプライヤーを特定することも可能である．よって，個人を特定する権限を持つ第三者が存在することになる．

取引サプライヤーをグループ登録する者は，登録しようとするグループメンバとして適切かどうかの審査と登録を依頼する必要がある．これらの審査と登録処理を行うような第三者の存在も必要である．

また，このようなトレーサビリティの中で，詳細情報を非公開にする必要がないサプライヤーも存在する．そのサプライヤーは，個人の署名により検証者に対して本人であることを証明すればよい．

以上をまとめると，本稿で提案する手法に必要なエンティティとして以下の 6 つを定義する．

**サプライヤー（S）：** 検証者に本人であることを証明する．

**プライベート・サプライヤー (PS)：** サプライヤーの中で，検証者に個人を特定されずに，グループメンバであることを証明する．証明機関からグループメンバに所属するための基準を満たしているかを審査され，証明書を受け取る．

**サプライヤー・マネージャー（SM）：** プライベート・サプライヤーのグループメンバ登録を証明機関に依頼する．

**証明機関（CA）：** 信頼できる第三者機関で，プライベート・サプライヤーが登録を要求するグループに適切かどうかを審査し，適切あればグループメンバに登録し，証明書を発行する．検証者にプライベート・サプライヤーがグループに属しているということを検証するための証明書を渡す．

**検証者（V）：** サプライヤーが本人であることを検証する．また，プライベート・サプライヤー正当なグループメンバであるかを検証する．プライベート・サプライヤーの特定を行いたい場合に，Auditor へ依頼する．

**Auditor（A）：** プライベート・サプライヤーの個人を特定することができる信頼できる第三者機関．検証者の依頼により，必要に応じて個人を特定する．

ここでは，証明機関はグループメンバ登録のための審査や，メンバ登録，証明書発行などを行う役割を持つ機関，Auditor はプライベート・サプライヤー個人を特定する役割を持つ機関と区別している．しかし，証明機関と Auditor の役割を持つ一つの第三者機関が存在すると考えることもできる．

## 4. 提 案 手 法

### 4.1 プロトコル

S1 から PS1，PS1 から PS$n$ までの $n$ 人の PS，さらに PS$n$ から S2（かつ SM）へ何らかのメッセージが送られ，そのメッセージを V が受け取るようなフローを考える．このとき，提案するプロトコルとして以下のような手順が必要である．

- 証明書の発行・通知
- 署名チェーンの生成
- 署名検証
- 署名者特定

これらの手順の詳細を以下に説明する．

**【証明書の発行・通知】（図 5）**

（1） SM(S2) が管理する PS1〜PS$n$ を，指定するグループに登録するよう CA に依頼する．

（2） CA は PS1〜PS$n$ がグループに適切かどうかを審査し，承認されれば各 PS に証明書を発行する．

（3） 各 PS は CA から発行された証明書を受け取ることにより，登録されたグループの署名を行うことができるようになる．

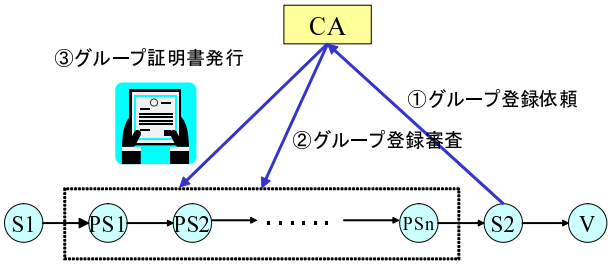


図 5 証明書の発行・通知

**【署名チェーンの生成】（図 6）**

署名チェーンとは，複数の署名者がメッセージに対して署名した署名文のことで，その署名方法として，多重署名などが存在する [4] [5]．ここでの署名チェーンも，基本的に多重署名のような既存技術を用いて作成できるものとする．

（1） S1 がメッセージ $M$ に署名する．$Sig_{S1}(M)$ とする．

（2） PS1 が S1 から受け取った署名付きメッセージ $Sig_{S1}(M)$ にグループ署名をする．グループメンバによる署名を $Sig_G$ とすると，以下のようになる．

$$Sig_G(Sig_{S1}(M)) \tag{1}$$

このとき，PS1 が S1 からの署名付きメッセージを受け取ると同時に，別の S である S1' からも署名付きメッセージ $Sig_{S1'}(M')$ を受け取るとすると，PS1 の署名文は以下のようになる．

$$Sig_G(Sig_{S1}(M), Sig_{S1'}(M')) \tag{2}$$

となる．これは，S1' が PS1' である場合も同様である．

（3） (2) と同様に，PS2 から PS$n$ がグループ署名をすると，署名チェーンは以下のようになる．

$$Sig_G(Sig_G(\cdots(Sig_G(Sig_{S1}(M)))\cdots)) \tag{3}$$

（4） 署名チェーン (3) に S2（SM）が署名をすると，以下のようになる．

$$Sig_{S2}(Sig_G(Sig_G(\cdots(Sig_G(Sig_{S1}(M)))\cdots))) \qquad (4)$$

検証者は，署名チェーン (4) を検証子として受け取り，署名の検証を行う．

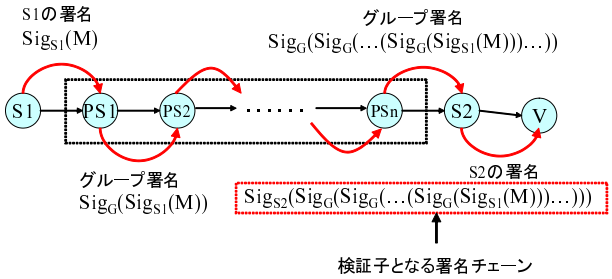


図 6　署名チェーンの生成

**【署名検証手順】（図 7）**

（1） CA に，「PS は SM が提示したグループに属している」ということを検証するための証明書，すなわちグループ公開鍵の送付を依頼し，受け取る．

（2） 署名チェーンから，S2 の公開鍵を用いて S2 であることを検証する．

（3） S2 の署名を除いた署名チェーンから，グループ公開鍵を用いて，PS1〜PS$n$ がグループメンバであることを検証する．

（4） $n$ 個のグループ署名を除いた署名チェーンから，S1 の公開鍵を用いて， S1 であることを検証する．

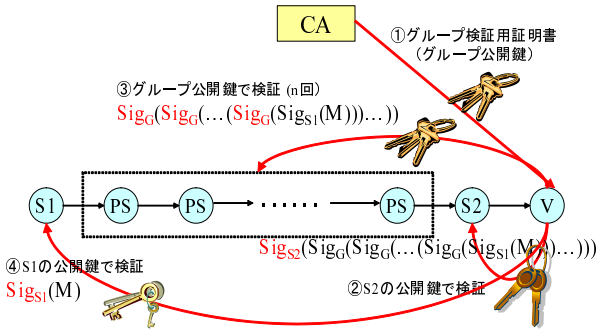


図 7　署名チェーンの検証

**【署名者特定手順】（図 8）**

（1） 検証者が Auditor にグループ署名の個人特定を依頼する．

（2） Auditor はグループ秘密鍵を用いて，グループ署名のチェーンから PS 個人と，PS 間の具体的な関連を特定する．

### 4.2　要件の検証

4.1 節で述べたプロトコルによって実現される検証可能性，非公開性，非公開解除可能性について考察する．

**【検証可能性】**

本手法によって，以下のことが検証可能である．

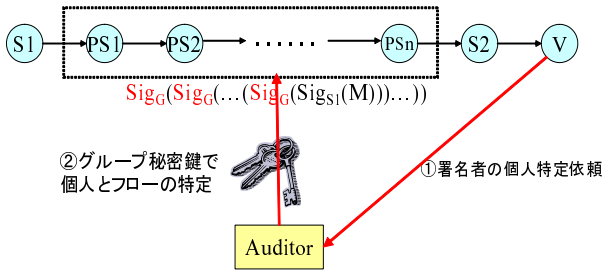


図 8　署名者の特定

- フローを作っている S や PS は，それぞれ次の S や PS に渡すメッセージに署名し，署名チェーンを作ることから，S であれば個人が，PS であればグループメンバが送信したメッセージであることが分かる．
- S の公開鍵やグループ公開鍵で署名チェーンを検証することにより，何人の S または PS が署名しているのかが分かることから，何人の S または PS を経たフローであるかが分かる．
- グループ公開鍵で署名チェーンを検証することによって，CA から承認されたグループメンバである PS がメッセージに署名していることが分かる．

**【非公開性】**

本手法によって，V が検証を行っても V に対して非公開性が保たれるのは以下のような項目である．

- PS はグループ署名を用いているので，正当なグループメンバであることは検証できるが，PS が PS1, PS2, ..., PS$n$ であることを特定することはできない．
- 署名チェーンの検証によって，S1 からある正当なグループメンバ PS へ，ある正当なグループメンバ PS から S2 へメッセージを送信していることは分かるが，S1 から PS1 へ送信し，PS$n$ から S2 へ送信していることは知ることができない．
- 署名チェーンによって，$n$ 人の正当なグループメンバ PS 間でのメッセージ送信が行われているかは分かるが，PS1 から PS2，PS2 から PS3, ..., PS$(n-1)$ から PS$n$ へ送信していることは知ることができない．

**【非公開解除可能性】**

本手法によって，権限を持つ Auditor のみが以下のように非公開性を解除することができる．非公開解除可能性が実現されることにより，何らかのトラブルが発生した場合に，原因を調査することができる．

- グループ秘密鍵を用いてグループ署名を検証することにより，V に知られることなく $n$ 人のグループメンバは，PS1, PS2, ..., PS$n$ であることが分かる．
- グループ秘密鍵を用いてグループ署名を検証することにより，V に知られることなく，PS1 から PS2, PS2 から PS3, ..., PS$(n-1)$ から PS$n$ へメッセージを送信していることが分かる．

以上のことから，本手法によって 2. 章で述べた要件を満たすようなトレーサビリティを実現することができる．

### 4.3　柔　軟　性

様々なサプライヤー間での取引において，一つのサプライ

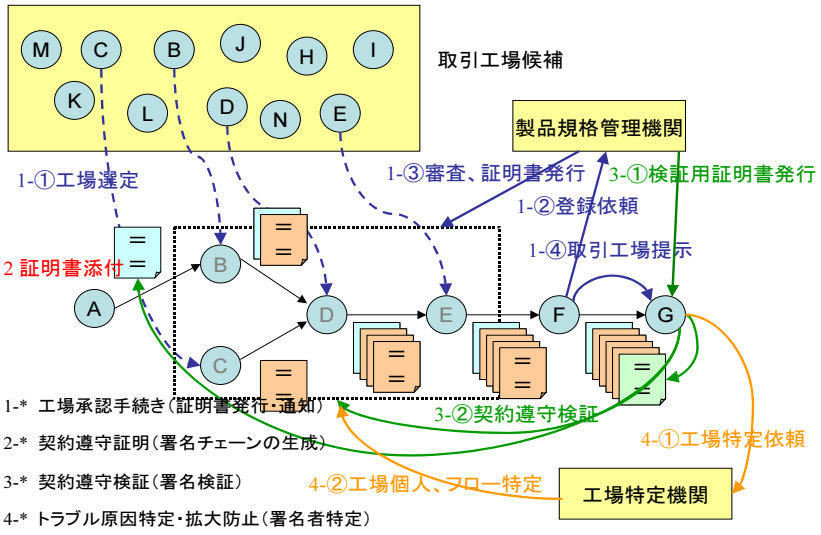


図8：実用例1　自動車の部品トレーサビリティへの適用

図 9　適用例：自動車部品のトレーサビリティ

ヤーの立場が，以下のように相手に応じて変わることは，頻繁に起こりうる状況である．

- 自分の取引サプライヤーを PS としたい．
- 自分があるサプライヤーの取引サプライヤーで，グループメンバ登録される．
- トレーサビリティにおける追跡対象者であるが，個人を特定されても問題がない．
- 自分が取引しているサプライヤーが，正当な処理，納品を行っているか検証したい．

このような状況においても，本プロトコルでは，状況に応じて同じサプライヤーが SM, PS, S, V と柔軟に変化することにより対応できることから，様々なトレーサビリティに対する検証を行うことが可能である．

## 5.　適　用　例

### 5.1　自動車部品トレーサビリティ

2.1 節で挙げた自動車部品のトレーサビリティのシナリオに本手法を適用する．登場するサプライヤーとサプライチェーンの構成は 2.1 節と同様で，これを 4.1 節で記述した手順に当てはめて説明する．また，自動車業界における証明機関，Auditor としてそれぞれ製品規格管理機関，工場特定機関という第三者機関が存在すると仮定する．

**製品規格管理機関：** 証明機関 CA
**工場 A（サプライヤー A）：** サプライヤー S1
**工場 B，C，D，E（サプライヤー B～E）：** プライベート・サプライヤー PS1, PS2, PS3, PS4
**工場 F（サプライヤー F）：** サプライヤー S2 かつサプライヤーマネージャー SM
**自動車ディーラー（サプライヤー G）：** 検証者 V
**工場特定機関：** Auditor

4.1 節で述べたプロトコルを適用した全体の流れを図 9 に示す．番号 1～4 は，それぞれ【工場承認手続き】,【契約遵守証明】,【契約遵守検証】,【トラブル原因特定・拡大防止】作業を表し，それぞれ 4.1 節の【証明書の発行・通知】,【署名チェーンの作成】,【署名検証】,【トラブル原因特定・拡大防止】の手順に該当する．番号①～④は，番号 1～4 のうちのある手順における作業順序である．例えば,「1-①工場選定」は，証明書発行・通知手順の 1 番目を表している．

以下に図 9 の各手順を詳しく述べる．

**【工場承認手続き（証明書発行・通知）】**

（1）　工場 F は，取引工場の中から,「日本の工場―製品品質レベル A 以上」のグループに登録できそうな候補である工場 B，C，D，E を選定する．

（2）　工場 F は，選定した工場 B～E を「日本の工場―製品品質レベル A 以上」のグループに登録するため，製品規格管理機関へ審査を依頼する．

（3）　製品規格管理機関は，工場 B～E の製品品質レベルを審査する．基準を満たしていれば,「日本の工場―製品品質レベル A 以上」のグループであることを示す証明書を発行する．

（4）　工場 F は，ディーラーと契約する際に，取引工場は製品品質レベル A 以上の日本の工場だけであることを提示する．

**【契約遵守証明（署名チェーンの生成）】**

（1）　工場 A は，自分の証明書を部品納品時に添付する．

（2）　工場 B は，工場 A から受け取った証明書とともに，製品規格管理機関で発行されたグループ証明書を部品納品時に添付する．

（3）　同様に，工場 C から工場 E まで受け取った証明書とともに，グループ証明書を部品納品時に添付する．

（4）　工場 F は，工場 E から受け取った証明書とともに，自分の証明書を自動車納品時に添付する．

証明書の添付方法については，後述する 5.2.1 項においても議論する．

**【契約遵守検証（署名検証）】**

（1）　自動車ディーラーは，製品規格管理機関から「製品品

質レベル A 以上の日本の工場である」ことを検証するために必要な証明書を受け取る．

（2） 自動車ディーラーは，納品時に受け取った添付証明書と，（1）で受け取った証明書を用いて，以下の項目を満たしているかを検証する．

- 工場 F から納入した自動車が，工場 A の部品を使っている．
- 工場 F が提示した「日本の工場―製品品質レベル A 以上」の取引工場から仕入，加工，組立を行っている．

署名検証の方針については，後述する 5.2.2 項においても議論する．

**【トラブル原因調査・拡大防止（署名者特定）】**

（1） 納入した自動車の部品に何らかのトラブルがあり，工場 F の取引工場を特定する必要がある場合は，ディーラーは工場特定機関に依頼し，工場特定機関が取引工場を特定し，原因を調査する．

（2） 調査の結果，トラブルが拡大する可能性がある場合は，取引工場の取引関係を検証し，納品先などを特定することにより，トラブルの拡大を防止する．

以上のプロトコルによって，工場 F の取引工場の詳細情報を自動車ディーラーに知られることなく，自動車ディーラーに対して取引の正当性を証明することができる．さらに，サプライチェーン間で，何らかのトラブルが発生した場合は，権限をもつ第三者によって，取引工場個人や工場間の具体的な関係を特定すると，自動車ディーラーはトラブルの原因を知ることができるとともに，トラブルの拡大を防止することができる．

### 5.2 議　　論

5.1 節で述べた契約遵守証明における証明書添付方法と，契約遵守検証における証明書の検証について議論する．さらに，証明機関と Auditor の信頼性についても議論する．

#### 5.2.1 証明書添付方法

証明書はグループ署名を行うことにより作成されることから，基本的には添付証明書はデジタルデータである．そこで添付方法としては，例えば以下のような方法が考えられる．

- 部品タグに署名を埋め込む
- デジタル納品書に署名し，納品先へ送信する
- サーバで署名チェーンを管理し，ディーラーが必要に応じてサーバから署名チェーンを取り出す

状況に応じて様々な添付方法を用いることができるため，本プロトコルを導入するサプライチェーンの性質や，システムの運用方針に応じて柔軟に対応することができる．

#### 5.2.2 証明書の検証

ディーラーは，自動車が納入されるたびに必ずしも証明書を検証する必要はない．工場 F は契約を遵守しているとある程度は信頼し，一定の期間ごと，あるいは何らかのトラブルが生じた場合に検証を行うというように，状況に応じて検証を行うことができる．つまり，納入時に毎回署名データの受信や検証を行う必要はないので，署名データの送信，検証コストにも考慮することができる．

#### 5.2.3 証明機関と Auditor

本手法では，工場の製品品質レベルを審査，保証するのは証明機関のみであるから，工場の製品品質レベルが本当に求められているレベルであるとみなすためには，証明機関の信頼性に大きく依存する．もし証明機関の信頼性が低ければ，工場の製品品質に何らかの問題があった際に，証明機関の審査そのものが問題とされる可能性がある．同様に，工場を特定する機関は Auditor ただ一つであるため，Auditor の信頼性が低ければ，工場の特定結果が信頼されない可能性がある．このことから，本手法が現実的に適用されるためには，3.2 節の証明機関，Auditor の説明においても述べたように，信頼できる第三者機関であることが重要である．

## 6. ま と め

トレーサビリティにおいて必要な検証可能性，非公開性，非公開解除可能性を実現する手法として，グループ署名を用いたプロトコルを提案した．本手法によって，追跡対象となるサプライヤーの詳細情報やサプライヤー間の具体的な関連などを秘匿しながら，処理や納品過程の正当性を検証することが可能になる．さらに，非公開解除可能性を実現する第三者によって，何らかのトラブルが生じた際にも対応することができる．

本手法を適用したトレーサビリティは，知られるとビジネス上で大きな不利益をもたらす可能性のある情報は非公開にする一方で，追跡者に対して品質の保証を証明することができる．また，複雑だが疎な関係にある現在のサプライチェーンにおいて，サプライヤーの立場が様々に変化する場合にも柔軟に対応することから，多くの分野において効果を発揮することができる．

## 文　　献


[1] 加藤岳久，岡田光司，吉田琢也，「プライバシを保護する匿名認証システムの開発」，CSS2003, pp.569-574, 2003.

[2] D. Chaum , E. van Heijst, ”Group Signature”, Adcanves in Cryptology - EUROCRYPTO ’91, pp.257-265, Springer-Verlag, 1991.

[3] Giuseppe Ateniese, J. Camenisch, Marc Joye, and Gene Tsudik, ”A Practical and Provably Secure Coalition-Resistant Group Signature Scheme”, In CRYPTO ’2000, pp.255-270, Springer-Verlag, 2000.

[4] M. Burmester, Yvo Desmedt, Hiroshi Doi, Masahiro Mambo, Eiji Okamoto, Mitsuru Tada, and Y. Yoshifuji, ”A structured elgamal-type multisignature scheme.”, In Advances in Cryptology-Proceedings of PKC’ 2000), Lecture Notes in Computer Science, pp.466-482, 2000.

[5] Shirow Mitomi and Atsuko Miyaji, ”A multisignature scheme with message flexibility, order flexibility and order verifiability”, In Proceedings of the 5th Australasian Conference on Information Security and Privacy, 2000.