

明 細 書

発明の名称：

流通管理装置、流通管理システム、及び流通管理方法

技術分野

[0001] 本発明は、流通管理装置、流通管理システム、及び流通管理方法に関する。

背景技術

[0002] ===参照による取り込み===

本出願は、2018年7月30日に出願された日本特許出願第2018-142396号の優先権を主張し、その内容を参照することにより、本出願に取り込む。

製品の製造プロセスにおける部品の調達、加工、製品の組み立て、製品の出荷、販売、利用者による製品の運用、利用及び保守、さらにその後の製品の二次利用、廃棄、及びリサイクルに至るまでのサプライチェーン全体において、製品の構成部品の来歴、流通経路、及び利用状況等の情報を追跡可能とする、トレーサビリティの要求が高まっている。この背景には、サプライチェーンがグローバルに分散化し流動化する中で、メーカーによるリコール対応、ユーザからのクレーム対応、製品の盗難及び偽造対応、並びに監査証跡の対応等、流通の正当性を証明するためのコストが増大していることが挙げられる。

[0003] これらの対応を効率的にするための技術として、例えば特許文献1には、多数の部品からなる製品に関する複雑な流通経路の記録を正しく記録し、効率的に検証可能とするために、電子署名をアイテム群に対してまとめて付与する方法が開示されている。

[0004] また、特許文献2には、サプライチェーン関与者に分散するトレーサビリティ情報に自在にアクセスすることを可能にすると共に、それらのトレーサビリティ情報へのアクセス権限を管理する方法が開示されている。

先行技術文献

特許文献

[0005] 特許文献1：特許4 1 1 1 5 2 9号公報

特許文献2：特開2 0 0 8－1 3 9 9 9 5号公報

発明の概要

発明が解決しようとする課題

[0006] ところで昨今では、製品の利用者は販売後の製品を利用又は消費するだけでなくこれを転売する傾向にあり、これによりフリーマーケットやオークション等の転売市場が拡大している。このような市場では、製品の所有者、利用方法、又は保管の状態等、製品の販売後の状況によって付加価値が増減するが、このような製品に関わる属性情報を正しく証明することは困難である。

[0007] また、購入した商品を単一の利用者が利用するだけでなく、他の利用者と共有するシェアリング市場も拡大しているが、このような市場では利用者が頻繁に変わるため、特定の利用者や製品（例えば、製品に対して問題のある利用をした者）を追跡又は特定することが難しかった。

[0008] このような製品に関わる属性情報の正しい証跡を全員で共有する方法として、昨今、ブロックチェーン技術の活用が提案されている。そこで、このブロックチェーン技術と、特許文献1、特許文献2の技術を活用することが考えられる。例えば、製品の転売において、所有者はサプライチェーンにおける当該製品のトレーサビリティ情報（例えば、所有者、転売先、価格等の情報）の証跡に基づいて現在価値を証明し、対価を設定して他の利用者に販売し、他方、購入者側もトレーサビリティ情報の証跡に基づいて購入することが考えられる。

[0009] しかしながら、このトレーサビリティ情報は、製品の所有者以外の者が無制限にアクセスできると個人情報の保護等の観点から問題が生じる。例えば、特許文献2には、トレーサビリティ情報の参照要求時に、取引関係マスタ

ーデータベースを参照して参照権限を確認するアクセス権限チェック部を備えることで、アクセス権限に応じた参照制御を行う方法が開示されているが、このアクセス権限の設定は固定的であり、個人情報の適切な保護が図られるとは限らない。

[0010] 本発明はこのような背景に鑑みてなされたものであり、その目的は、製品の流通過程に関する情報に対するアクセス権を適切に設定することが可能な流通管理装置、流通管理システム、及び流通管理方法を提供することにある。

課題を解決するための手段

[0011] 上記課題を解決するための、本発明の一つは、流通管理装置であって、所定の端末から、所定の製品の流通における各プロセスのうち完了したプロセス及びその関係者の情報を含むトランザクションデータを受信するトランザクション受信部と、前記受信したトランザクションデータに基づき、前記完了したプロセス、その関係者、及びその関係者が有する所定のアクセス権の間の関係の情報であるアクセス権限情報を生成するアクセス権限情報生成部と、所定の端末から、前記製品の流通におけるプロセスに関する情報提供要求を受信する情報提供要求受信部と、前記受信した情報提供要求の送信元がアクセス権を有する、前記流通におけるプロセスの情報を、前記アクセス権限情報に基づき特定するアクセス権判定部と、前記特定したプロセスに関する情報を、前記情報提供要求を送信した端末に送信する情報送信部と、を備える。

発明の効果

[0012] 本発明によれば、製品の流通過程に関する情報に対するアクセス権を適切に設定することができる。

図面の簡単な説明

[0013] [図1]本実施形態のトレーサビリティシステムの構成の一例を示す図である。

[図2]各ノードが備えるハードウェアの一例を示す図である。

[図3]本実施形態のサプライチェーンに係る製品の流通経路の一例を示す図で

ある。

[図4]トレーサビリティ情報管理サーバが備える機能の一例を説明する図である。

[図5]アクセス権限更新ルールマスタの一例を示す図である。

[図6]ユーザクライアントが備える機能の一例を示す図である。

[図7]トランザクション送信処理の一例を説明するフロー図である。

[図8]製造トランザクションデータの一例を示す図である。

[図9]納品トランザクションデータの一例を示す図である。

[図10]販売トランザクションデータの一例を示す図である。

[図11]利用トランザクションデータの一例を示す図である。

[図12]保管トランザクションデータの一例を示す図である。

[図13]サプライチェーン情報更新処理の一例を示すフロー図である。

[図14]トレーサビリティ情報の一例を示す図である。

[図15]アクセス権限情報データベースの一例を示す図である。

[図16]トレーサビリティ情報提供処理の一例を説明するフロー図である。

発明を実施するための形態

[0014] 以下、本発明の実施形態について図面を用いて説明する。

<<システム構成>>

図1は、本実施形態の流通管理システムであるトレーサビリティシステム100の構成の一例を示す図である。トレーサビリティシステム100は、所定の製品に関するサプライチェーンシステムにおける当該製品の流通経路（トレーサビリティ）を管理する情報処理システムである。トレーサビリティシステム100は、複数のトレーサビリティ情報管理サーバ101（流通管理装置）と、少なくとも1以上のユーザクライアント102の各ノードと、認証基盤システム200とを含んで構成されている。

[0015] トレーサビリティ情報管理サーバ101は、サプライチェーンにおけるトランザクション及びトランザクションのトレーサビリティに関する情報（以下、サプライチェーン情報という。）を管理している。

- [0016] 複数のトレーサビリティ情報管理サーバ101により、ブロックチェーンによる分散台帳システムが構成され、製品の流通におけるプロセスを示すトランザクションデータに係るブロックチェーンデータを各ノード（トレーサビリティ情報管理サーバ101）が共有している。ここで、ブロックチェーンデータは、複数のブロックデータが時系列的に連結してなり、各ブロックデータは、複数のトランザクションと直前のブロックデータのハッシュ値とからなる。各ノードは、所定の電子署名を付したトランザクションデータを生成し、生成したトランザクションデータに対する合意形成を行い、所定のタイミング（例えば、所定の時間間隔）で、複数のトランザクションデータをまとめたブロックデータを生成する。この結果生成されたブロックチェーンデータが、各ノードで共有される。
- [0017] 本実施形態では、製品の流通におけるプロセスには、そのプロセスを実行する本人、及び任意的に一人以上の関係者が関与している。ここで、関係者とは、例えば、製品の製造、流通、又は販売に関わる企業の従業員（例えば、製造工程における加工や組み立てに従事する作業員、受発注業務を行う調達部門担当者、流通プロセスにおける物流事業者、販売事業者等）、監査機関の従業員（監査者）、及び製品を購入又は利用する消費者（例えば、製品購入者、転売先の購入者、シェアリング等における利用者、修理事業者、リサイクル事業者等を含む）である。
- [0018] ユーザクライアント102は、所定のユーザ（例えば、サプライチェーンのプロセスを実行した本人及び関係者等）が使用する端末であり、トレーサビリティ情報管理サーバ101にアクセスすることにより、サプライチェーン情報の登録及び参照を行う。
- [0019] 認証基盤システム200は、トランザクションデータに付与されている電子署名を検証する。
- [0020] トレーサビリティ情報管理サーバ101、ユーザクライアント102、及び認証基盤システム200の間は、例えば、LAN（Local Area Network）、WAN（Wide Area Network）、インターネット、又は専用線等の、有線又

は無線の通信ネットワーク 103 によって通信可能に接続されている。

[0021] なお、図 2 は、各ノードが備えるハードウェアの一例を示す図である。各ノードは、CPU (Central Processing Unit) などのプロセッサ 41 と、RAM (Random Access Memory)、ROM (Read Only Memory) 等の主記憶装置 42 と、HDD (Hard Disk Drive)、SSD (Solid State Drive) 等の補助記憶装置 43 と、キーボード、マウス、タッチパネルなどからなる入力装置 44 と、モニタ (ディスプレイ) 等からなる出力装置 45 と、他のノードと通信を行う通信装置 46 とを備える。

[0022] <<サプライチェーンに係る流通経路>>

図 3 は、本実施形態のサプライチェーンに係る製品の流通経路の一例を示す図である。本実施形態の流通経路は、所定の製造業者 (製造企業) が所定の加工を行うことにより所定の部材を作成する加工プロセス (s1)、作成した各部材を組み立てることにより所定の製品を製造する製造プロセス (s3) を含む。また、この流通経路は、製造業者が製造した製品を所定の納品先 (例えば、配送業者、販売業者) に納品する納品プロセス (s5)、その後、納品先が消費者に製品を譲渡 (例えば、販売) する販売プロセス (s7) を含む。また、この流通経路は、消費者がその製品を利用する利用プロセス及びこれを第三者に保管させる保管プロセスを含む (s9)。さらに、この流通経路は、製品の譲渡を受けた消費者がその製品を他の消費者に譲渡 (例えば、販売) する販売プロセス (s11) を含む。

[0023] ところで、これらの各プロセスの情報を本サプライチェーンの関係者全員に提供する (開示する) ことは、個人情報の保護、セキュリティ等の観点から好ましくない。そこで、本実施形態のトレーサビリティシステム 100 は、流通経路の各プロセスの情報に対するアクセス権原をその種類に応じて設定することで、必要な関係者のみに必要な限度で各プロセスの情報が提供されるようにする。

[0024] <<機能>>

次に、トレーサビリティシステム 100 における各ノード (情報処理装置

）が備える機能について説明する。

[0025] <トレーサビリティ情報管理サーバ>

図4は、トレーサビリティ情報管理サーバ101が備える機能の一例を説明する図である。トレーサビリティ情報管理サーバ101は、トランザクションデータの履歴がブロックチェーンデータの形態で記録されているトランザクションログ104と、完了したトランザクションとその関係者等の情報が記録されているトレーサビリティ情報900と、トランザクションデータに対するアクセス権限が記録されているアクセス権限情報1000と、トランザクション、関係者、及びアクセス権限の間の所与の関係が記録されているアクセス権限更新ルールマスタ1100とを記憶している。

[0026] (アクセス権限更新ルールマスタ)

ここで、図5は、アクセス権限更新ルールマスタ1100の一例を示す図である。アクセス権限更新ルールマスタ1100は、トランザクションの種別（プロセスの種別）を示す情報が格納されるトランザクション種別1101、トランザクション種別1101が示す種別のプロセスにおける本人（当該プロセスを実行する者）が有するアクセス権に関する情報が格納される本人1103、トランザクション種別1101が示す種別のプロセスにおける関係者のうち製品の移転先の相手に関する情報が格納される移転先1105、及び、トランザクション種別1101が示す種別のプロセスにおける関係者のうち監査者に関する情報が格納される監査者1107の各項目を有する。

[0027] ここで、監査者とは、例えば、認証機関や会計法人を始めとする、トランザクションを監査する必要のある者である。

[0028] また、移転先の相手は、例えば、トランザクションデータに係るプロセスが受発注、販売、譲渡、利用等のプロセスの場合はそれぞれ、購入者、譲渡先、利用者等である。

[0029] 本人1103、移転先1105、及び監査者1107にはそれぞれ、アクセス権に関する情報が格納されており、具体的には、流通経路における下流

側に対するアクセス権（フォワードアクセス権）に関する情報が格納されるフォワードアクセス権 1108 と、流通経路における上流側に対するアクセス権（バックアクセス権）に関する情報であるバックアクセス権 1109 とが格納されている。フォワードアクセス権 1108 及びバックアクセス権 1109 には、例えば、アクセス権の有無の情報、流通経路のどのプロセスまでに権限を付与するかといった情報が格納される。

[0030] 図 5 の例では、例えばトランザクション種別が「加工」の場合、本人である加工業者には製造者責任があるため、下流側については納入先への「納品」までに限定したアクセス権を付与し、上流側には現プロセスに至るまでのプロセスについて知る権利があるため、無制限のアクセス権を付与している。監査者にも同様に現プロセスに至るまでの監査者責任として上流側のアクセス権のみを付与している。なお、本人は、自身が行ったプロセスに対するアクセス権を有する。以上は、トランザクション種別が「組み立て」の場合も同様である。

[0031] トランザクション種別が「納品」の場合、製造者である本人は販売代理店に納めた以降の情報を追跡すべきでないため、フォワードアクセス権は付与しない（「非付与」）とする一方、製造者責任があるため、納品に至るまでの全てのプロセスに対するアクセス権を付与する。また、移転先である販売代理店には、購入者への説明責任を果たすため、上流側及び下流側を含む全てのプロセスへのアクセス権を付与する。

[0032] また、トランザクション種別が「販売」の場合、本人である販売者は前記のとおり購入者への説明責任を果たすため、上流側及び下流側を含む全てのプロセスへのアクセス権を付与する。

[0033] トランザクション種別が「販売（消費者間）」（消費者間での販売）の場合は、本人である販売元（転売元）のアクセス権は下流側及び上流側共に抹消し、移転先である販売先（購入者）には、1 段階（1 プロセス）のフォワードアクセス権、及び無制限のバックアクセス権を付与している。これにより、転売元が購入者への転売後、その購入者が更に誰に販売したか等を追跡

できないように、アクセス権を設定することができる。

- [0034] トランザクション種別が「利用」の場合には、本人である利用者のみが参照できるようにするため、その本人に対してのみアクセス権を付与する。
- [0035] トランザクション種別が「保管」の場合には、移転先及び監査者に対してバックアクセス権を付与する。ただし、本人である保管者本人に対しては１プロセス分のみフォワードアクセス権を付与する。
- [0036] 図４に戻り、トレーサビリティ情報管理サーバ１０１は、アクセス権限情報１０００を記憶するアクセス権限マスタ記憶部１１１と、トランザクション受信部１１３と、トランザクション検証部１１５と、各データベースにアクセスするデータアクセス部１１７と、情報提供要求受信部１１９と、アクセス権判定部１２１と、情報送信部１２３とを備える。
- [0037] アクセス権限マスタ記憶部１１１は、製品の流通における各プロセスの種類と、各プロセスの各関係者が有するアクセス権との関係を記憶した情報であるアクセス権限マスタ（アクセス権限更新ルールマスタ１１００）を記憶する。
- [0038] なお、アクセス権限マスタ（アクセス権限更新ルールマスタ１１００）における各プロセスの各関係者は、プロセスを実行する者、プロセスによる製品の移転先の相手、又は、プロセスの監査者のうち少なくともいずれかを含む。
- [0039] また、アクセス権は、アクセス権の保有者である関係者が、その関係者により完了したプロセスよりも後に完了したプロセスに対するアクセス権であるフォワードアクセス権、又は、アクセス権の保有者である関係者が、その関係者により完了したプロセスよりも前に完了したプロセスに対するアクセス権であるバックアクセス権を含む。
- [0040] トランザクション受信部１１３は、所定の端末（ユーザクライアント１０２）から、所定の製品の流通における各プロセスのうち完了したプロセス及びその関係者の情報を含むトランザクションデータを受信する。
- [0041] トランザクション検証部１１５は、トランザクション転送部１１５１と、

書き込み試行部 1153 と、結果受信部 1155 を備える。

- [0042] トランザクション転送部 1151 は、トランザクションデータを受信した場合、受信したトランザクションデータを他の流通管理装置（トレーサビリティ情報管理サーバ 101）に転送する。
- [0043] 書き込み試行部 1153 は、受信したトランザクションデータに基づく所定のデータの生成を行い、その生成結果の情報を生成する。
- [0044] 結果受信部 1155 は、他の流通管理装置（トレーサビリティ情報管理サーバ 101）が生成した、前記の転送されたトランザクションデータに基づく所定のデータの生成結果を他の流通管理装置（トレーサビリティ情報管理サーバ 101）から受信する。
- [0045] データアクセス部 117 は、アクセス権限情報生成部 1171、及びトランザクション共有部 1173 を備える。
- [0046] アクセス権限情報生成部 1171 は、トランザクション受信部 113 が受信したトランザクションデータに基づき、完了したプロセス、その関係者、及びその関係者が有する所定のアクセス権の間の関係の情報であるアクセス権限情報 1000 を生成する。
- [0047] 例えば、アクセス権限情報生成部 1171 は、アクセス権限マスタ（アクセス権限更新ルールマスタ 1100）に基づき、アクセス権限情報 1000 として、完了したプロセスの種類、その関係者、及びその関係者が有するアクセス権の間の関係を記憶した情報を生成する。
- [0048] また、アクセス権限情報生成部 1171 は、結果受信部 1155 が受信した生成結果のうち所定数の結果が一致する場合に、アクセス権限情報 1000 を生成する。
- [0049] トランザクション共有部 1173 は、前記所定数の結果が一致した場合に、受信したトランザクションデータと過去のトランザクションデータのハッシュ値とを含むブロックデータを生成し、生成したブロックデータを含むブロックチェーンデータを他の流通管理装置（トレーサビリティ情報管理サーバ 101）と共有する。

- [0050] 情報提供要求受信部 119 は、所定の端末（ユーザクライアント 102）から、製品の流通におけるプロセスに関する情報提供要求を受信する。
- [0051] アクセス権判定部 121 は、情報提供要求受信部 119 が受信した情報提供要求の送信元がアクセス権を有する、流通におけるプロセスの情報を、アクセス権限情報 1000 に基づき特定する。
- [0052] 情報送信部 123 は、情報提供要求受信部 119 が特定したプロセスに関する情報を、情報提供要求を送信した端末（ユーザクライアント 102）に送信する。

[0053] <ユーザクライアント>

図 6 は、ユーザクライアント 102 が備える機能の一例を示す図である。ユーザクライアント 102 は、トランザクションデータを生成するトランザクション生成部 131、トランザクションデータに付与する電子署名を生成する電子署名生成部 133、トランザクションデータをトレーサビリティ情報管理サーバ 101 に送信するトランザクション送信部 135、及び、サプライチェーンシステムにおける製品の流通経路に関する情報（以下、トレーサビリティ関連情報という）を取得するトレーサビリティ関連情報取得部 137 を備える。

- [0054] また、ユーザクライアント 102 は、トランザクションデータに対して付与される電子署名である、所定の秘密鍵 139 を記憶している。
- [0055] 以上に説明した各情報処理装置の機能は、各情報処理装置のハードウェアによって、もしくは、各情報処理装置のプロセッサ 41 が、主記憶装置 42 や補助記憶装置 43 に記憶されている各プログラムを読み出して実行することにより実現される。
- [0056] また、これらのプログラムは、例えば、二次記憶デバイスや不揮発性半導体メモリ、ハードディスクドライブ、SSDなどの記憶デバイス、又は、ICカード、SDカード、DVDなどの、情報処理装置で読み取り可能な非一時的データ記憶媒体に格納される。
- [0057] <<処理>>

次に、トレーサビリティシステム１００において行われる処理について説明する。トレーサビリティシステム１００は、ユーザクライアント１０２がトランザクションを送信する処理（以下、トランザクション送信処理という。）と、トレーサビリティ情報管理サーバ１０１が受信したトランザクションに基づきサプライチェーン情報を更新する処理（以下、サプライチェーン情報更新処理という。）と、トレーサビリティ情報管理サーバ１０１がユーザクライアント１０２に対し、サプライチェーン関連情報を提供する処理（以下、サプライチェーン情報提供処理という。）とを実行する。

[0058] <トランザクション送信処理>

図７は、トランザクション送信処理の一例を説明するフロー図である。この処理は、例えば、流通過程における各プロセスが完了したことを契機に開始される。

[0059] まず、ユーザクライアント１０２は、完了したプロセスに関するトランザクションデータを生成し、生成したトランザクションデータに、電子署名を付与する。

[0060] 例えば、完了したプロセスが完了の証跡を残すべきプロセスである場合（例えば、製造プロセス、又は利用プロセスである場合）は、ユーザクライアント１０２は、完了したプロセスを示す情報（完了プロセス情報という。）を含むトランザクションデータを生成する（s 301 a）。そして、ユーザクライアント１０２は、生成したトランザクションデータに、本人の電子署名（ユーザクライアント１０２の秘密鍵による電子署名）を付与する（s 302 a）。その後は、s 304 の処理が行われる。

[0061] 他方、例えば、完了したプロセスが所有権の移転や利用権の移転の証跡を残すべきプロセスである場合（例えば、納品プロセス、販売プロセス、又は保管プロセスである場合）、ユーザクライアント１０２は、移転の内容を示す情報（以下、移転情報という。）を含むトランザクションデータを生成する（s 301 b）。そして、ユーザクライアント１０２は、生成したトランザクションデータに、本人（移転元）の電子署名を付与する（s 302 b）

。さらに、ユーザクライアント１０２は、当該トランザクションデータに、移転先の電子署名を付与する（ｓ３０３ｂ）。その後はｓ３０４の処理が行われる。

[0062] ｓ３０４においてユーザクライアント１０２は、完了したプロセスに監査者がいるか否かをアクセス権限更新ルールマスタ１１００により判定する。完了したプロセスに監査者がいる場合には（ｓ３０４：ＹＥＳ）、ユーザクライアント１０２は、トランザクションデータに、その監査者の電子署名を付与する（ｓ３０４）。完了したプロセスに監査者がいない場合には（ｓ３０４：ＮＯ）、ｓ３０６の処理が行われる。

[0063] 次に、ユーザクライアント１０２は、生成したトランザクションデータを、トレーサビリティ情報管理サーバ１０１に送信する（ｓ３０６）。以上でトランザクション送信処理は終了する。

[0064] なお、監査者及び移転先は複数存在してもよい。また、付与される監査者及び移転先の電子署名は、予めユーザクライアント１０２に記録されてよいし、ユーザクライアント１０２が、当該監査者及び移転先に係るユーザクライアント１０２に電子署名を要求してもよい。例えば、ユーザクライアント１０２は、監査者及び移転先に係るユーザクライアント１０２に電子署名の要求を送信し、当該ユーザクライアント１０２から、電子署名を受信する。

[0065] <トランザクションデータ>

ここで、トランザクション送信処理において生成されるトランザクションデータについて説明する。

[0066] （製造トランザクションデータ）

図８は、製品の製造プロセスが完了した際に生成されるトランザクションデータ（製造トランザクションデータ）の一例を示す図である。製造トランザクションデータ４００は、トランザクションの種類（「製造」）を示す情報であるトランザクション種別４０１、当該トランザクションの発生タイミングの情報である発生日時４０２、製造者（本人）を示す情報である作業者ＩＤ４０３、使用される機械を示す情報である作業機械ＩＤ４０４、製造作

業の内容を示す情報である作業内容405、製造における加工前の部材（構成部材）を示す情報である構成部材406、製造における加工後の部材（完成部材）を示す情報である完成部材ID407の各情報を有する。また、製造トランザクションデータ400には、本人（作業者、製造者等）の電子署名である作業者署名408、及び、監査者の電子署名である監査者署名409が付与されている。なお、製造プロセスには、例えば、製造工程における部材の加工や製品の組み立てが含まれる。製造トランザクションデータ400は、例えば、熟練工が加工を行ったことを証明することができる。

[0067]（納品トランザクションデータ）

図9は、製品の納品プロセスが完了した際に生成されるトランザクションデータ（納品トランザクションデータ）の一例を示す図である。納品トランザクションデータ500は、トランザクションの種別（納品）を示す情報であるトランザクション種別501、トランザクションの発生タイミングの情報である発生日時502、納品の発注者（本人又は移転元）の情報である発注者ID503、納品の納品先（移転先）の情報である受注者ID504、納品対象の部材の情報である対象部材ID505、納品対象の部材の価格の情報である価格506、及び、納品の決済の情報である決済ID507の各情報を含む。また、納品トランザクションデータ500には、発注者（本人又は移転元）の電子署名である発注者署名508、及び受注者（移転先）の電子署名である受注者署名509が付与される。

[0068]（販売トランザクションデータ）

図10は、製品の販売プロセスが完了した際に生成されるトランザクションデータ（販売トランザクションデータ）の一例を示す図である。販売トランザクションデータ600は、トランザクションの種別の情報（すなわち、「販売」を示す情報）であるトランザクション種別601、トランザクションの発生タイミングの情報である発生日時602、製品の販売者（本人又は移転元）の情報である販売者ID603、製品の購入者（移転先）の情報である購入者ID604、製品の情報である製品ID605、及び、製品の価

格の情報である価格606などの項目を含む。また、販売トランザクションデータ600には、販売者の電子署名である販売者署名607、及び購入者の電子署名である購入者署名608が付与される。

[0069] 納品トランザクションデータ500や販売トランザクションデータ600は、例えば、部品のリコール対応時に現在の所有者を特定したり、利用者からのクレームに対してどの部品が使われているかを特定したりするために利用できる。

[0070] (利用トランザクションデータ)

図11は、製品の利用プロセスが完了した際に生成されるトランザクションデータ(利用トランザクションデータ)の一例を示す図である。利用トランザクションデータ700は、トランザクションの種別の情報(すなわち、「利用」を示す情報)であるトランザクション種別701、トランザクションにおける製品の利用期間である期間702、製品の所有者の識別子である所有者ID703、及び、製品の識別子である製品ID704の各情報を含む。また、利用トランザクションデータ700には、所有者(本人)の電子署名である所有者署名705が付与される。利用トランザクションデータ700は、例えば、有名人が製品を所有したことの証明として利用することで、製品を付加価値を付けて販売する際の裏づけの情報とすることができる。

[0071] (保管トランザクションデータ)

図12は、製品の保管プロセスが完了した際に生成されるトランザクションデータ(保管トランザクションデータ)の一例を示す図である。保管トランザクションデータ800は、トランザクションの種別の情報(すなわち、「保管」を示す情報)であるトランザクション種別801、製品の保管期間の情報である期間802、製品の所有者の情報である所有者ID803、製品の保管者の情報である保管者ID804、製品の情報である製品ID805の各情報を含む。また、保管トランザクションデータ800には、移転元(本人又は所有者)の電子署名である所有者署名806及び、移転先(保管者)の電子署名である保管者署名807が付与される。保管トランザクシ

ンデータ 800 は、例えば、適切な温度管理でワインを保管したことを証明するデータとして利用することができる。

[0072] <サプライチェーン情報更新処理>

図 13 は、サプライチェーン情報更新処理の一例を示すフロー図である。トレーサビリティ情報管理サーバ 101 は、ユーザクライアント 102 のいずれかからトランザクションデータを受信すると (s801)、トランザクションデータの検証を行う (s802)。

[0073] 具体的には、例えば、トレーサビリティ情報管理サーバ 101 は、受信したトランザクションデータに付帯している電子署名に対する検証を、認証基盤システム 200 に実行させる。すなわち、トレーサビリティ情報管理サーバ 101 は、他のトレーサビリティ情報管理サーバ 101 と、トランザクションデータに関する合意形成処理を行うことにより、トランザクションデータの正当性を確認する。合意形成処理は、例えば、以下のように行われる。

[0074] まず、トレーサビリティ情報管理サーバ 101 は、他のトレーサビリティ情報管理サーバ 101 にトランザクションデータを転送する (s802a)。転送先の各トレーサビリティ情報管理サーバ 101 は、トランザクションデータに対して所定の書き込み処理を試行してその結果の情報を生成する。

[0075] トレーサビリティ情報管理サーバ 101 は、他の各トレーサビリティ情報管理サーバ 101 が生成した結果の情報をそれぞれ受信し (s802b)、それらの結果のうち一定数以上 (又は一定割合以上。例えば過半数。) が一致する場合に、s801 で受信したトランザクションデータを承認し、そうでない場合には承認しない。

[0076] このように、複数のトレーサビリティ情報管理サーバ 101 が行う合意形成処理により、特定の中央管理者や中央管理サーバが存在しなくても、トランザクションデータの正当性を検証し、データの改竄等の不正のリスクを低減することができる。

[0077] このような処理によって、トランザクションデータを承認しないと判定された場合 (s802c: NO)、トレーサビリティ情報管理サーバ 101 は

、受信したトランザクションデータを承認しない旨の情報をユーザクライアント102に送信し(s804)、サプライチェーン管理情報更新処理は終了する(s809)。

[0078] 他方、トランザクションデータを承認する場合(s802c: YES)、トレーサビリティ情報管理サーバ101は、そのトランザクションデータの内容を一時的に記憶し、その後、トランザクションデータに関するブロックチェーンデータをトランザクションログ104に書き込むと共に、他のトレーサビリティ情報管理サーバ101と当該ブロックチェーンデータを共有する(s805)。

[0079] 具体的には、例えば、トレーサビリティ情報管理サーバ101は、所定のタイミング(例えば、10分おき)が到来するまで、承認した複数のトランザクションデータを複数蓄積し、蓄積したトランザクションデータ群に、時系列的に一つ前の、トランザクションデータに係るブロックデータのハッシュ値を含めたブロックデータを生成する。これによりトレーサビリティ情報管理サーバ101は、ハッシュ値を介した、トランザクションデータに係るブロックチェーンデータを生成する。そして、トレーサビリティ情報管理サーバ101は、生成したブロックチェーンデータをトランザクションログ104に書き込むと共に、当該ブロックチェーンデータを他の全てのトレーサビリティ情報管理サーバ101に送信する。これにより、ブロックチェーンデータが各トレーサビリティ情報管理サーバ101で共有される。

[0080] 以上により、トランザクションデータの履歴を改竄不能な状態でトレーサビリティ情報管理サーバ101間で共有することが可能となる。

[0081] さらに、トレーサビリティ情報管理サーバ101は、受信したトランザクションデータに基づき、トレーサビリティ情報900を生成又は更新する(s806)。その後、トレーサビリティ情報900は他のトレーサビリティ情報管理サーバ101と共有される。

[0082] <トレーサビリティ情報900>

図14はトレーサビリティ情報900の一例を示す図である。トレーサビ

リティ情報 900 は、各トランザクションデータ（各プロセス）をリスト化したテーブルであり、トランザクションの識別子であるトランザクション ID 901、トランザクションの入力情報（後述）であるインプット 902、トランザクションの出力情報（後述）であるアウトプット 903、トランザクションの種別の情報であるトランザクション種別 904、本人（例えば、製造者、移転元）の情報である本人 ID 905、本人以外（例えば、移転先）の情報である移転先 ID 906、及び、監査者の情報である監査者 ID 907 の各項目を有する、1 以上のレコードで構成される。

[0083] なお、インプット 902 には、例えば、トランザクションが製造トランザクションの場合は部品の情報（部品 ID）が格納される（複数の部品が存在する場合もある）。アウトプット 903 には、例えば、トランザクションが製造トランザクションの場合は製品の情報（製品 ID）が格納される。なお、加工トランザクションや販売トランザクション等、製品のみを対象とするトランザクションの場合は、アウトプット 903 にのみ情報が格納され、インプット 902 には情報が格納されない。

[0084] トレーサビリティ情報管理サーバ 101 は、トレーサビリティ情報 900 を参照することにより、例えばある部品がどの製品に使われており、その製品の所有者がどのように変遷しているかを容易に追跡（フォワードトレース）することができる。また、トレーサビリティ情報管理サーバ 101 は、ある利用者が利用している製品に含まれる部品を遡って検索（バックトレース）することもできる。

[0085] また、トレーサビリティ情報管理サーバ 101 は、種別の異なるトランザクションデータをまとめてトレーサビリティ情報 900 として記憶することにより、トランザクションデータの検索速度を向上させることができる。例えば、あるブロックチェーンシステムが、トレーサビリティ情報 900 のようなデータ構造の情報をキーバリューストアで格納するコンポーネントを備えている場合に、そのようなブロックチェーンシステムに効率よく対応することができる。

[0086] 図13に戻り、トレーサビリティ情報管理サーバ101は、アクセス権限更新ルールマスタ1100を参照することにより、アクセス権限情報1000を生成又は更新する(s807)。その後、アクセス権限情報1000は他のトレーサビリティ情報管理サーバ101と共有される。以上でサプライチェーン情報更新処理は終了する(s808)。

[0087] <アクセス権限情報1000>

図15は、アクセス権限情報1000の一例を示す図である。アクセス権限情報1000は、各プロセスにおける本人が、その下流側のプロセス(時間的に後のプロセス)に対するデータのフォワードアクセス権、及び、その上流側のプロセス(時間的に前のプロセス)に対するバックアクセス権をそれぞれ有しているかを記録した情報である。アクセス権限情報1000には、例えば、トランザクションが発生する毎にレコードが追加され、又はレコードの更新が行われる。

[0088] アクセス権限情報1000は、トランザクションの識別子であるトランザクションID1001、トランザクションの種別であるトランザクション種別1002、トランザクションにおける本人の識別子である対象者ID1003、本人のフォワードアクセス権(アクセス権限更新ルールマスタ1100より取得)の保有の有無を示すフォワードアクセス権1004、及び本人のバックアクセス権(アクセス権限更新ルールマスタ1100より取得)の保有の有無を示すバックアクセス権1005の各項目を有する、1以上のレコードで構成されている。

[0089] <トレーサビリティ情報提供処理>

次に、図16は、トレーサビリティ情報提供処理の一例を説明するフロー図である。なお、この処理は、例えば、トレーサビリティ情報管理サーバ101がアクセス権限情報1000を生成した後に開始される。

[0090] トレーサビリティ情報管理サーバ101は、ユーザクライアント102から、トレーサビリティ情報の提供の要求(以下、情報提供要求という。)を受信する(s1201)。なお、本実施形態では、情報提供要求は、送信元

の情報（例えば、ユーザIDやユーザクライアント102の識別子）と、情報の提供を要求する、送信元が完了させたプロセスの情報（以下、要求トランザクションという。）と、製品の情報とを含む情報に、秘密鍵による電子署名が付与されたものとする。

[0091] トレーサビリティ情報管理サーバ101は、受信した情報提供要求の正当性を検証する（s1202）。具体的には、例えば、トレーサビリティ情報管理サーバ101は、認証基盤システム200に、情報提供要求における電子署名の正当性の確認を要求する。

[0092] 正当性が確認されなかった場合は（s1203：NO）、トレーサビリティ情報管理サーバ101は、ユーザクライアント102に対して、正当性が確認できない旨の情報（NGメッセージ）を送信し（s1204）、トレーサビリティ情報提供処理は終了する（s1205）。

[0093] 正当性が確認された場合は（s1203：YES）、トレーサビリティ情報管理サーバ101は、要求トランザクションの送信元が有するアクセス権限（フォワードアクセス権及びバックアクセス権）を取得する（s1206）。具体的には、例えば、トレーサビリティ情報管理サーバ101は、アクセス権限情報1000のうちトランザクションID1001に要求トランザクションの情報が格納されているレコードにおけるフォワードアクセス権1004及びバックアクセス権1005を取得する。

[0094] 送信元がバックアクセス権を有していない場合には（s1207：NO）、後述するs1209の処理が行われ、送信元がバックアクセス権を有している場合には（s1207：YES）、トレーサビリティ情報管理サーバ101は、要求トランザクションよりも上流側のトランザクションの情報を取得する（s1208）。具体的には、例えば、トレーサビリティ情報管理サーバ101は、s1206で取得したレコードのうち、要求トランザクションのよりも上流側のトランザクションを特定し、特定したトランザクションが格納されているトレーサビリティ情報900のレコードの内容を取得する。その後は、s1209の処理が行われる。

- [0095] s 1 2 0 9において、送信元がフォワードアクセス権を有していない場合には（s 1 2 0 9 : N O）、後述するs 1 2 1 1の処理が行われ、送信者がフォワードアクセス権を有している場合には（s 1 2 0 9 : Y E S）、トレーサビリティ情報管理サーバ1 0 1は、要求トランザクションよりも下流側のトランザクションの情報を取得する（s 1 2 1 0）。具体的には、例えば、トレーサビリティ情報管理サーバ1 0 1は、s 1 2 0 6で取得したレコードのうち、要求トランザクションのよりも下流側のトランザクションを特定し、特定したトランザクションが格納されているトレーサビリティ情報9 0 0のレコードの内容を取得する。その後は、s 1 2 1 1の処理が行われる。
- [0096] s 1 2 1 1においてトレーサビリティ情報管理サーバ1 0 1は、s 1 2 0 8で取得した、要求トランザクションよりも上流側のトランザクションの情報と、s 1 2 1 0で取得した、要求トランザクションよりも上流側のトランザクションの情報とを結合したデータ（以下、送信情報という。）を生成する。
- [0097] トレーサビリティ情報管理サーバ1 0 1は、生成した送信情報をユーザクライアント1 0 2に送信し（s 1 2 1 2）、トレーサビリティ情報提供処理は終了する（s 1 2 1 3）。他方、ユーザクライアント1 0 2は、受信した送信情報を画面等に表示する（s 1 2 1 5）。
- [0098] 以上のように、本実施形態の流通管理装置（トレーサビリティ情報管理サーバ1 0 1）は、ユーザクライアント1 0 2から受信したトランザクションデータに基づき、所定の製品の流通（サプライチェーン）における各プロセスのうち完了したプロセス、その関係者、及びその関係者が有する所定のアクセス権の間の関係の情報であるアクセス権限情報1 0 0 0を生成する一方、ユーザクライアント1 0 2から受信した情報提供要求に基づき、送信元がアクセス権を有する、完了したプロセスに関する情報をアクセス権限情報1 0 0 0に基づき特定し、特定した情報を情報提供要求を送信した端末に送信する。
- [0099] すなわち、トレーサビリティ情報管理サーバ1 0 1は、サプライチェーン

における各プロセスの関係者とアクセス権の関係を記憶しておき、ユーザからの情報提供要求に対しては、そのユーザがアクセス権を有するプロセスについてのみ情報を提供するので、製品の流通過程に関する情報に対するアクセス権を適切に設定することができる。例えば、トレーサビリティ情報管理サーバ101は、製品や部品に関するトレーサビリティに対するアクセス権限管理を動的かつ正確に行うことができる。

[0100] 以上の各実施形態の説明は、本発明の理解を容易にするためのものであり、本発明を限定するものではない。本発明はその趣旨を逸脱することなく、変更、改良され得ると共に本発明にはその等価物が含まれる。

[0101] 例えば、本実施形態では、サプライチェーンにおいて加工、組み立て（製造）、利用、保管、譲渡（販売）等のプロセスを管理と対象としたが、それ以外の工程についても同様に管理可能である。

[0102] また、本実施形態でアクセス権は、フォワードアクセス権及びバックアクセス権があるものとしたが、それ以外でも、個別のプロセスに対してアクセス権を設定するといったことも可能である。

[0103] また、本実施形態では関係者は、製品（部品）の移転先の者、又は監査者であるものとしたが、それ以外の関係者（利害関係人）を追加してもよい。

[0104] 以上の本明細書の記載により、少なくとも次のことが明らかにされる。すなわち、本実施形態の流通管理装置においては、前記製品の流通における各プロセスの種類と、前記各プロセスの各関係者が有するアクセス権との関係を記憶した情報であるアクセス権限マスタを記憶するアクセス権限マスタ記憶部を備え、前記アクセス権限情報生成部は、前記アクセス権限マスタに基づき、前記アクセス権限情報として、前記完了したプロセスの種類、その関係者、及びその関係者が有するアクセス権の間の関係を記憶した情報を生成する、としてもよい。

[0105] このように、製品の流通における各プロセスの種類と、各プロセスの各関係者が有するアクセス権との関係を記憶したアクセス権限マスタ（アクセス権限更新ルールマスタ1100）に基づき、完了したプロセスの種類、その

関係者、及びその関係者が有するアクセス権の間の関係を記憶したアクセス権限情報 1000 を生成することにより、例えば、プロセスを実行した者の情報アクセス権を適切に管理することができる。

[0106] また、本実施形態の流通管理装置においては、前記アクセス権限マスタにおける前記各プロセスの各関係者は、当該プロセスを実行する者、当該プロセスによる製品の移転先の相手、又は、当該プロセスの監査者のうち少なくともいずれかを含む、としてもよい。

[0107] このように、アクセス権限更新ルールマスタ 1100 が、製品の流通プロセスを実行する本人、製品の移転先、又は監査者の情報を有していることで、取引相手や監査を行う者が存するような様々な種類のプロセス（トランザクション）を適切に管理することができる。

[0108] また、本実施形態の流通管理装置においては、前記アクセス権は、当該アクセス権の保有者である関係者が、当該関係者により完了したプロセスよりも後に完了したプロセスに対するアクセス権であるフォワードアクセス権、又は、当該アクセス権の保有者である関係者が、当該関係者により完了したプロセスよりも前に完了したプロセスに対するアクセス権であるバックアクセス権を含む、としてもよい。

[0109] このように、アクセス権がフォワードアクセス権又はバックアクセス権を含むことで、サプライチェーンにおける上流側から下流側へのプロセス全般を管理することができる。

[0110] また、本実施形態においては、所定の端末から、所定の製品の流通における各プロセスのうち完了したプロセス及びその関係者の情報を含むトランザクションデータを受信するトランザクション受信部と、前記受信したトランザクションデータに基づき、前記完了したプロセス、その関係者、及びその関係者が有する所定のアクセス権の間の関係の情報であるアクセス権限情報を生成するアクセス権限情報生成部と、所定の端末から、前記製品の流通におけるプロセスに関する情報提供要求を受信する情報提供要求受信部と、前記受信した情報提供要求の送信元がアクセス権を有する、前記流通における

プロセスの情報を、前記アクセス権限情報に基づき特定するアクセス権判定部と、前記特定したプロセスに関する情報を前記情報提供要求を送信した端末に送信する情報送信部と、を備える流通管理装置を複数含んで構成され、前記流通管理装置は、前記トランザクションデータを受信した場合、受信したトランザクションデータを他の流通管理装置に転送するトランザクションデータ転送部と、前記他の流通管理装置が生成した、前記転送されたトランザクションデータに基づく所定のデータの生成結果を受信する結果受信部とを備え、前記アクセス権限情報生成部は、前記生成した生成結果及び前記受信した生成結果のうち所定数の結果が一致する場合に、前記アクセス権限情報を生成する、流通管理システム、としてもよい。

[0111] このように、流通管理装置が、受信したトランザクションデータを他の流通管理装置に転送すると共に、他の流通管理装置が生成した、そのトランザクションデータに基づく所定のデータの生成結果を受信し、受信した生成結果のうち所定数の結果が一致する場合に、アクセス権限情報1000を生成する、といった合意形成の処理を行うことで、トランザクションデータの正当性を検証し、データの改竄等の不正のリスクを低減することができる。このように、ブロックチェーン技術を活用すれば、改竄不能でかつ記録者を確実に証明可能な、トレーサビリティの情報を管理することが可能となる。

[0112] また、本実施形態の流通管理装置においては、前記流通管理装置は、前記所定数の結果が一致した場合に、前記受信したトランザクションデータと過去のトランザクションデータのハッシュ値とを含むブロックデータを生成し、生成したブロックデータを含むブロックチェーンデータを他の流通管理装置と共有するトランザクション共有部を備える、としてもよい。

[0113] このように、各流通管理装置が、トランザクションデータによるブロックチェーンデータを他の流通管理装置と共有するといったブロックチェーンシステムを構成していることで、トランザクションデータを大量かつセキュアに管理することができる。

符号の説明

[0114] 100 トレーサビリティシステム、101 トレーサビリティ情報管理サーバ、102 ユーザクライアント、113 トランザクション受信部、1171 アクセス権限情報生成部、121 アクセス権判定部、123 情報送信部