

明 細 書

発明の名称：

通信システム、ポリシー管理装置、通信方法およびプログラム

技術分野

[0001] （関連出願についての記載）

本発明は、日本国特許出願：特願２０１１－２０４４８７号（２０１１年９月２０日出願）の優先権主張に基づくものであり、同出願の全記載内容は引用をもって本書に組み込み記載されているものとする。

[0002] 本発明は、通信システム、ポリシー管理装置、通信方法およびプログラムに関し、特に、ネットワークに配置された転送ノードによりパケットを転送して通信を実現する通信システム、ポリシー管理装置、通信方法およびプログラムに関する。

背景技術

[0003] 特許文献１、非特許文献１、２において、オープンフロー（Open Flow）という技術が記載されている。オープンフローでは、通信をエンドツーエンドのフローとして捉え、フロー単位で経路制御、障害回復、負荷分散および最適化が行われる。

[0004] 非特許文献２に仕様化されているオープンフロースイッチは、制御装置に相当するオープンフローコントローラとの通信用のセキュアチャネルを備えている。オープンフロースイッチは、オープンフローコントローラから追加または書き換えを適宜指示されるフローテーブルに従って動作する。

[0005] フローテーブルには、フロー毎に、パケットヘッダと照合するマッチングルール（ヘッダフィールド、Header Field）と、フロー統計情報（カウンタ、Counters）と、処理内容を定義したアクション（Actions）と、の組が定義される（図３参照）。

[0006] 例えば、オープンフロースイッチは、パケットを受信すると、フローテーブルから、受信パケットのヘッダ情報に適合するマッチングルール（図３の

ヘッダフィールド参照)を持つエントリを検索する。

[0007] 検索の結果、受信パケットに適合するエントリが見つかった場合には、オープンフロースイッチは、フロー統計情報（カウンタ）を更新するとともに、受信パケットに対して、当該エントリのアクションフィールドに記述された処理内容（例えば、指定ポートからのパケット送信、フラッディング、廃棄等）を実施する。

[0008] 一方、検索の結果、受信パケットに適合するエントリが見つからなかった場合には、オープンフロースイッチは、セキュアチャネルを介して、オープンフローコントローラに対して受信パケットを転送し、受信パケットの送信元・送信先に基づいたパケットの経路の決定を依頼する。また、オープンフロースイッチは、この経路に従ったパケット転送を実現するためのフローエントリをオープンフローコントローラから受け取って、フローテーブルを更新する。

[0009] このように、オープンフロースイッチは、フローテーブルに格納されたエントリを処理規則として用いることで、パケット転送を行う。

先行技術文献

特許文献

[0010] 特許文献1：国際公開第2008/095010号

非特許文献

[0011] 非特許文献1：Nick McKeownほか7名、“OpenFlow：Enabling Innovation in Campus Networks,” March 14, 2008 [online], [平成23年9月7日検索]，インターネット〈URL：<http://www.openflowswitch.org/documents/openflow-wp-latest.pdf>〉。

非特許文献2：“OpenFlow Switch Specification” Version 1.1.0 Implemented (Wire Protocol 0x02) February 28, 2011、[

online], [平成23年9月7日検索], インターネット〈URL : <http://www.openflowswitch.org/documents/openflow-spec-v1.1.0.pdf>〉.

発明の概要

発明が解決しようとする課題

[0012] 上記の特許文献および非特許文献の開示内容は、本書に引用をもって繰り込み記載されているものとする。以下の分析は、本発明によって与えられたものである、

[0013] 特許文献1に記載されたオープンフローコントローラ、すなわち、オープンフローの制御装置は、新規フロー発生時に、アクセス制御ルールを参照してパーミッションチェックを行ない、その後、経路を計算することによりアクセス制御を行う（特許文献1の[0052]参照）。

[0014] ここで、新規フロー発生時に参照するアクセス制御ルールは、ポリシー管理装置によって生成されたアクセス制御リスト（ACL : Access Control List）を受け取ることで更新される。

[0015] ポリシー管理装置がACLを生成する際には、アクセス元のホストとアクセス先のネットワーク資源の情報が必要となる。

[0016] ネットワーク管理者やアクセス制御を要望するユーザが、これらの情報をポリシー管理装置に手作業で入力しても、アクセス制御は可能となる。しかし、かかる方法によると、ネットワーク管理者やユーザの手間が大きく、大規模なネットワークや、頻繁にホストやネットワーク資源の接続状態が変化する環境においてアクセス制御を行うことは困難となる。

[0017] 一方、これらの情報の収集作業をシステムで自動化することができれば、ネットワーク管理者やユーザの手間を大幅に削減できる。このとき、大規模なネットワークや、頻繁にホストやネットワーク資源の接続状態が変化するような環境において、簡単かつ現実的な手間および時間でアクセス制御を行うことが可能となる。

[0018] また、ポリシー管理装置に対して、アクセス制御内容を設定するためには

、ホストやネットワーク資源の情報を指定したアクセス制御ポリシーを用いる。

[0019] ポリシー管理装置は、アクセス制御ポリシーに基づいてACLを生成する。

[0020] アクセス制御ポリシーに対して、ホストやネットワーク資源の情報を指定する際は、ホストやネットワーク資源のネットワーク環境内での識別子となる現時点でのアドレス情報等を指定する必要がある。

[0021] アクセス制御の対象となるホストやネットワーク資源の場所や接続状態が変化した場合には、ホストやネットワーク資源のネットワーク上からの生滅やアドレスの変化が発生する。アクセス制御を正しく行うには、その変化に応じてリアルタイムにアクセス制御ポリシーを更新し、更新されたアクセス制御ポリシーから新たにACLを生成して、制御装置の持つアクセス制御ルールを更新しなければならない。

[0022] ネットワーク管理者やアクセス制御を要望するユーザが、これらの情報をポリシー管理装置に手作業で入力しても、アクセス制御は可能となる。しかし、かかる方法によると、ネットワーク管理者やユーザの手間が大きく、大規模なネットワークや、頻繁にホストやネットワーク資源の接続状態が変化するような環境においてアクセス制御を行うことは困難となる。

[0023] 一方、これらの情報の指定作業をシステムで半自動化することにより、一旦指定すれば、その後は自動で変化に追従するような抽象化された分かりやすい指定方法を、ネットワーク管理者やユーザに対して提供することができれば、ネットワーク管理者やユーザの手間を大幅に削減することができる。このとき、大規模なネットワークや、頻繁にホストやネットワーク資源の接続状態が変化するような環境において、簡単かつ現実的な手間および時間でアクセス制御を行うことが可能となる。

[0024] しかしながら、上記のような解決を図るには、アクセス元のホストの情報やアクセス先のネットワーク資源の情報について、現在の接続状態をリアルタイムに収集したり、アクセス制御ポリシーに記載された抽象的な指定に基

づいて、具体的なホストやネットワーク資源の情報を探し出す機能が必要とされる。

[0025] そこで、機器が大量に存在し接続状態が頻繁に変化する場合や、ユーザが大量に存在し接続状態が頻繁に変化する場合においても、リアルタイムにアクセス制御を更新できるようにすることが要望される。本発明の目的は、かかる要望に寄与する通信システム、ポリシー管理装置、通信方法およびプログラムを提供することにある。

課題を解決するための手段

[0026] 本発明の第1の視点に係る通信システムは、
処理規則に従ってパケットを処理する複数の転送ノードと、
前記複数の転送ノードを制御する制御装置と、
前記複数の転送ノードのいずれかに接続されたホストを使用するユーザを認証する認証装置と、
アクセス制御対象のホストの識別子とホストが接続された転送ノードの識別子とを紐付ける第1の紐付け手段、および／または、アクセス制御対象のホストの識別子とホストを使用するユーザの識別子とを紐付ける第2の紐付け手段を有し、転送ノードの識別子、および／または、ユーザの識別子を用いてアクセス制御対象のホストを特定するアクセス制御ポリシーを保持するポリシー管理装置と、を備え、
前記複数の転送ノードは、それぞれ、自身に接続されたホストの識別子と自身の識別子との組を前記ポリシー管理装置に送信し、
前記認証装置は、前記複数の転送ノードのいずれかに接続されたホストの識別子とユーザの識別子との組を前記ポリシー管理装置に送信し、
前記ポリシー管理装置は、前記アクセス制御ポリシーを参照し、前記複数の転送ノードにいずれかに接続されたホストがアクセス制御対象である場合には、アクセス制御の内容をアクセス制御リストとして前記制御装置に通知し、
前記制御装置は、前記アクセス制御リストに応じて前記処理規則を生成し

て、前記複数の転送ノードに設定する。

[0027] 本発明の第2の視点に係るポリシー管理装置は、

処理規則に従ってパケットを処理する複数の転送ノードと、アクセス制御リストに応じて該処理規則を生成して該複数の転送ノードに設定する制御装置と、該複数の転送ノードのいずれかに接続されたホストを使用するユーザを認証する認証装置と、を備えた通信システムにおけるポリシー管理装置であって、

アクセス制御対象のホストの識別子とホストが接続された転送ノードの識別子とを紐付ける第1の紐付け手段、および／または、アクセス制御対象のホストの識別子とホストを使用するユーザの識別子とを紐付ける第2の紐付け手段と、

転送ノードの識別子、および／または、ユーザの識別子を用いてアクセス制御対象のホストを特定するアクセス制御ポリシーを保持するアクセス制御ポリシー記憶部と、を備え、

前記複数の転送ノードのそれぞれから、自身に接続されたホストの識別子と自身の識別子との組を受信し、

前記複数の転送ノードのいずれかに接続されたホストの識別子とユーザの識別子との組を前記認証装置から受信し、

前記アクセス制御ポリシーを参照し、前記複数の転送ノードにいずれかに接続されたホストがアクセス制御対象である場合には、アクセス制御の内容を前記アクセス制御リストとして前記制御装置に通知する。

[0028] 本発明の第3の視点に係る通信方法は、

複数の転送ノードと、該複数の転送ノードを制御する制御装置と、該複数の転送ノードのいずれかに接続されたホストを使用するユーザを認証する認証装置と、転送ノードの識別子、および／または、ユーザの識別子を用いてアクセス制御対象のホストを特定するアクセス制御ポリシーを保持するポリシー管理装置と、を備えた通信システムにおける通信方法であって、

前記複数の転送ノードが、それぞれ、自身に接続されたホストの識別子と

自身の識別子との組を前記ポリシー管理装置に送信する工程と、

前記認証装置が、前記複数の転送ノードのいずれか接続されたホストの識別子とユーザの識別子との組を前記ポリシー管理装置に送信する工程と、

前記ポリシー管理装置が、アクセス制御対象のホストの識別子とホストが接続された転送ノードの識別子とを紐付ける工程、および／または、

アクセス制御対象のホストの識別子とホストを使用するユーザの識別子とを紐付ける工程と、

前記アクセス制御ポリシーを参照し、前記複数の転送ノードにいずれかに接続されたホストがアクセス制御対象である場合には、アクセス制御の内容をアクセス制御リストとして前記制御装置に通知する工程と、

前記制御装置が、前記アクセス制御リストに応じてパケットの処理規則を生成して、前記複数の転送ノードに設定する工程と、

前記複数の転送ノードが前記処理規則に従ってパケットを処理する工程と、を含む。

[0029] 本発明の第4の視点に係る通信方法は、

処理規則に従ってパケットを処理する複数の転送ノードと、アクセス制御リストに応じて該処理規則を生成して該複数の転送ノードに設定する制御装置と、該複数の転送ノードのいずれかに接続されたホストを使用するユーザを認証する認証装置と、を備えた通信システムにおいて、転送ノードの識別子、および／または、ユーザの識別子を用いてアクセス制御対象のホストを特定するアクセス制御ポリシーを保持するポリシー管理装置が、

アクセス制御対象のホストの識別子とホストが接続された転送ノードの識別子とを紐付ける工程、および／または、

アクセス制御対象のホストの識別子とホストを使用するユーザの識別子とを紐付ける工程と、

前記複数の転送ノードのそれぞれから、自身に接続されたホストの識別子と自身の識別子との組を受信する工程と、

前記複数の転送ノードのいずれかに接続されたホストの識別子とユーザの

識別子との組を前記認証装置から受信する工程と、

前記アクセス制御ポリシーを参照し、前記複数の転送ノードにいずれかに接続されたホストがアクセス制御対象である場合には、アクセス制御の内容を前記アクセス制御リストとして前記制御装置に通知する工程と、を含む。

[0030] 本発明の第5の視点に係るプログラムは、

処理規則に従ってパケットを処理する複数の転送ノードと、アクセス制御リストに応じて該処理規則を生成して該複数の転送ノードに設定する制御装置と、該複数の転送ノードのいずれかに接続されたホストを使用するユーザを認証する認証装置と、を備えた通信システムにおいて、転送ノードの識別子、および／または、ユーザの識別子を用いてアクセス制御対象のホストを特定するアクセス制御ポリシーを保持するポリシー管理装置に設けられたコンピュータに対して、

アクセス制御対象のホストの識別子とホストが接続された転送ノードの識別子とを紐付ける処理、および／または、

アクセス制御対象のホストの識別子とホストを使用するユーザの識別子とを紐付ける処理と、

前記複数の転送ノードのそれぞれから、自身に接続されたホストの識別子と自身の識別子との組を受信する処理と、

前記複数の転送ノードのいずれかに接続されたホストの識別子とユーザの識別子との組を前記認証装置から受信する処理と、

前記アクセス制御ポリシーを参照し、前記複数の転送ノードにいずれかに接続されたホストがアクセス制御対象である場合には、アクセス制御の内容を前記アクセス制御リストとして前記制御装置に通知する処理と、を実行させる。なお、プログラムは、非ランジエントなコンピュータ読み取り可能な記録媒体に記録されたプログラム製品として提供することができる。

発明の効果

[0031] 本発明に係る通信システム、ポリシー管理装置、通信方法およびプログラムによると、機器が大量に存在し接続状態が頻繁に変化する場合や、ユーザ

が大量に存在し接続状態が頻繁に変化する場合においても、リアルタイムにアクセス制御を更新することが可能となる。

図面の簡単な説明

[0032] [図1]実施形態に係る通信システムの構成を一例として示すブロック図である。

[図2]実施形態に係る通信システムの動作を一例として示すシーケンス図である。

[図3]オープンフロー（非特許文献2）のフローテーブルに格納されるエントリの構成を示す図である。

発明を実施するための形態

[0033] はじめに、本発明の概要について説明する。なお、この概要に付記する図面参照符号は、専ら理解を助けるための例示であり、本発明を図示の態様に限定することを意図するものではない。

[0034] 図1を参照すると、本発明の通信システムは、処理規則に従ってパケットを処理する複数の転送ノード（200A～200C）と、複数の転送ノードを制御する制御装置（300）と、複数の転送ノードのいずれかに接続されたホスト（100A、100B）を使用するユーザを認証する認証装置（310A～310C）と、アクセス制御対象のホストの識別子とホストが接続された転送ノードの識別子とを紐付ける第1の紐付け手段（トポロジ情報紐付け手段324）、および／または、アクセス制御対象のホストの識別子とホストを使用するユーザの識別子とを紐付ける第2の紐付け手段（認証情報紐付け手段323）を有し、転送ノードの識別子、および／または、ユーザの識別子を用いてアクセス制御対象のホストを特定するアクセス制御ポリシーを保持するポリシー管理装置（320）と、を備えている。複数の転送ノード（200A～200C）は、それぞれ、自身に接続されたホストの識別子と自身の識別子との組をポリシー管理装置（320）に送信する。認証装置（310A～310C）は、複数の転送ノードのいずれかに接続されたホスト（100A、100B）の識別子とユーザの識別子との組をポリシー管

理装置（３２０）に送信する。ポリシー管理装置（３２０）は、アクセス制御ポリシーを参照し、複数の転送ノードにいずれかに接続されたホストがアクセス制御対象である場合には、アクセス制御の内容をアクセス制御リストとして制御装置（３００）に通知する。制御装置（３００）は、アクセス制御リストに応じて処理規則を生成して、複数の転送ノード（２００Ａ～２００Ｃ）に設定する。

[0035] ここで、処理規則は、処理対象パケットを特定するための照合規則と、該照合規則に適合するパケットに適用する処理内容とを対応付けたものであってもよい。また、複数の転送ノード（２００Ａ～２００Ｃ）は、それぞれ、自身に接続されたホストの識別子と自身の識別子との組を、制御装置（３００）を経由してポリシー管理装置（３２０）に送信してもよい。制御装置（３００）は、複数の転送ノード（２００Ａ～２００Ｃ）のいずれかに接続されたホストの識別子と該転送ノードの識別子との組をトポロジ情報として保持し、アクセス制御リストに応じたパケットの処理規則を該トポロジ情報に基づいて生成してもよい。

[0036] 本発明では、制御装置が転送ノードを集中制御するオープンフローのような通信システムを用いて、アクセス元のホストやアクセス先のネットワーク資源の状態を取得することで、それらの情報をポリシー管理装置に受け渡し、変化のあったホストやネットワーク資源に関するアクセス制御内容を自動的に更新し、抽象的なアクセス制御ポリシー記述に対して該当する具体的なホストやネットワーク資源を自動的に抽出してアクセス制御内容を更新する。

[0037] 本発明によれば、全く別の機能として存在する、ホストやネットワーク資源等の機器に関するネットワーク制御に必要な管理機能と、ユーザの識別に必要な管理機能とを、簡便かつ自然に繋ぐ方法を提供することができるため、機器が大量に存在し接続状態が頻繁に変化する場合や、ユーザが大量に存在し接続状態が頻繁に変化する場合においても、それら別用途の管理機能そのものを、ポリシーから生成されるＡＣＬ情報の更新のトリガ、兼、更新す

べき情報の取得元として利用することで、両者を繋いで新たなアクセス元・アクセス先の指定方法を提供し、管理者や個々のユーザがアクセス制御ポリシーを多大な手間をかけて更新することなく、リアルタイムにアクセス制御を更新することが可能となる。

[0038] 本発明において、下記の形態が可能である。

[0039] [形態 1]

上記第 1 の視点に係る通信システムのとおりである。

[0040] [形態 2]

前記処理規則は、処理対象パケットを特定するための照合規則と、該照合規則に適合するパケットに適用する処理内容とを対応付けたものであってもよい。

[0041] [形態 3]

前記複数の転送ノードは、それぞれ、自身に接続されたホストの識別子と自身の識別子との組を、前記制御装置を経由して前記ポリシー管理装置に送信してもよい。

[0042] [形態 4]

前記制御装置は、前記複数の転送ノードのいずれかに接続されたホストの識別子と該転送ノードの識別子との組をトポロジ情報として保持し、前記アクセス制御リストに応じたパケットの処理規則を該トポロジ情報に基づいて生成してもよい。

[0043] [形態 5]

前記アクセス制御ポリシーは、アクセス制御対象のホストを特定するために、所定の場所に設置された転送ノードの識別子のリストを含んでいてもよい。

[0044] [形態 6]

前記アクセス制御ポリシーは、アクセス制御対象のホストを特定するために、所定の所属、所定の勤務地、所定の権限階層、および、所定の担当プロジェクトのうちの少なくともいずれかに該当するユーザの識別子のリストを

含んでいてもよい。

[0045] [形態 7]

上記第2の視点に係るポリシー管理装置のとおりである。

[0046] [形態 8]

上記第3の視点に係る通信方法のとおりである。

[0047] [形態 9]

上記通信方法において、前記処理規則は、処理対象パケットを特定するための照合規則と、該照合規則に適合するパケットに適用する処理内容とを対応付けたものであってもよい。

[0048] [形態 10]

上記通信方法において、前記複数の転送ノードは、それぞれ、自身に接続されたホストの識別子と自身の識別子との組を、前記制御装置を経由して前記ポリシー管理装置に送信してもよい。

[0049] [形態 11]

上記通信方法において、前記制御装置は、前記複数の転送ノードのいずれかに接続されたホストの識別子と該転送ノードの識別子との組をトポロジ情報として保持し、前記アクセス制御リストに応じたパケットの処理規則を該トポロジ情報に基づいて生成してもよい。

[0050] [形態 12]

上記通信方法において、前記アクセス制御ポリシーは、アクセス制御対象のホストを特定するために、所定の場所に設置された転送ノードの識別子のリストを含んでいてもよい。

[0051] [形態 13]

上記通信方法において、前記アクセス制御ポリシーは、アクセス制御対象のホストを特定するために、所定の所属、所定の勤務地、所定の権限階層、および、所定の担当プロジェクトのうちの少なくともいずれかに該当するユーザの識別子のリストを含んでいてもよい。

[0052] [形態 14]

上記第４の視点に係る通信方法のとおりである。

[0053] [形態１５]

上記第５の視点に係るプログラムのとおりである。

[0054] (実施形態)

一実施形態に係る通信システムについて、図面を参照して説明する。図１は、本実施形態に係る通信システムの構成を一例として示す図である。

[0055] 図１を参照すると、通信システムは、認証装置３１０Ａ～３１０Ｃ、ネットワーク資源６００Ａ～６００Ｃ、ホスト１００Ａ～１００Ｃ、転送ノード２００Ａ～２００Ｃ、制御装置３００、および、ポリシー管理装置３２０を備えている。

[0056] 通信システムは、会議室群、居室群、サーバプールから成る３つの拠点を含む。認証装置３１０Ａ、ネットワーク資源６００Ａおよび転送ノード２００Ａは、会議室群に設けられている。認証装置３１０Ｂ、ネットワーク資源６００Ｂおよび転送ノード２００Ｂは、居室群に設けられている。認証装置３１０Ｃ、ネットワーク資源６００Ｃおよび転送ノード２００Ｃは、サーバプールに設けられている。ホスト１００Ａは、会議室群に設けられた転送ノード２００Ａにアクセスする。一方、ホスト１００Ｂは、居室群に設けられた転送ノード２００Ｂにアクセスする。

[0057] まず、本実施形態における用語について説明する。ここでは、一例として、会議室群におけるホスト１００Ａ、認証装置３１０Ａ、転送ノード２００Ａ、ネットワーク資源６００Ａについて説明するが、居室群およびサーバプールについても、同様である。

[0058] <認証装置>

認証装置３１０Ａは、ホスト１００Ａや、ホスト１００Ａを使用しているユーザを認証する。認証装置３１０Ａは、認証手続の一貫として、ホスト１００Ａのアドレスを管理し、認証済みホストに対してアドレスの振出しを行うようにしてもよい。

[0059] 図１に示すように、通信システムに対して複数の認証装置３１０Ａ～３１

OCを設置するようにしてもよい。ただし、1つの認証装置が、ネットワーク全体の認証手続を管理するようにしてもよい。

[0060] <ネットワーク資源>

ネットワーク資源600Aは、ネットワーク経由で利用するアプリケーションサーバ等に相当する。ただし、ネットワーク資源600Aは、ユーザが有するホストを含んでもよい。例えば、あるユーザの端末に格納されたファイル等の資源を、他のユーザからアクセス・共有する場合には、ネットワーク資源600Aにホストが含まれる。また、ネットワーク資源600Aは、認証装置310Aによる認証後でなければ利用できないプロトコルや、認証装置310Aによる認証後でなければアクセス制御ルールで定義できないプロローを利用するような、認証装置310A以外の認証装置も含む。

[0061] <ホスト>

ホスト100Aは、拠点等のネットワークに接続して使用する、ユーザの端末となるコンピュータ、または、ネットワークに接続して使用するプリンタ、ストレージ等の周辺機器に相当する。なお、新規に接続されたネットワーク資源600Aも、ホスト100Aとして扱うことができる。

[0062] <ホスト管理情報>

制御装置300は、「ホスト管理情報」を記憶する。ホスト管理情報は、転送ノート200Aに接続されているホスト100A(ネットワーク資源600Aを含む)に関する管理情報である。ホスト管理情報には、例えば、ホスト100AのMAC(Media Access Control)アドレスと、ホスト100AのIP(Internet Protocol)アドレスと、ホスト100Aが接続されている転送ノート200Aの識別子と、ホスト100Aが接続されている転送ノート200Aのコネクタの識別子との組を含む。

[0063] <認証情報>

認証装置310Aは、「認証情報」を収集・管理する。認証情報は、ユーザやホスト100Aを特定する情報である。認証情報は、ユーザがホスト1

００Ａをネットワークと接続・切断するにあたって、ユーザやホスト１００Ａの認証を行った際に得られる。認証情報は、例えば、ホスト１００ＡのＭＡＣアドレスと、ホスト１００ＡのＩＰアドレスと、ホスト１００Ａを使用しているユーザＩＤとの組を含む。

[0064] <認証情報変化通知>

認証装置３１０Ａは、収集して得た認証情報の変化について、「認証情報変化通知」としてポリシー管理装置３２０に通知する。通知される情報は、例えば、ホスト１００ＡのＭＡＣアドレスと、ホスト１００ＡのＩＰアドレスと、ホスト１００Ａを使用しているユーザＩＤと、ホスト１００Ａの接続／切断の別との組を含む。

[0065] また、認証装置３１０Ａは、ユーザＩＤに付随して、ユーザの所属、勤務地、権限階層、担当プロジェクト等のユーザに関する様々な情報を管理する。

[0066] なお、上述の認証情報も、例えば、ホスト１００ＡのＭＡＣアドレスと、ホスト１００ＡのＩＰアドレスと、ホスト１００Ａを使用しているユーザＩＤとの組の他に、当該ユーザＩＤに対応するユーザに関する上述の様々な情報を含んでいてもよい。

[0067] <トポロジ情報>

制御装置３００は、「トポロジ情報」を収集する。トポロジ情報は、転送ノード２００Ａと、そこに接続および切断されたホスト１００Ａやネットワーク資源６００Ａの、設置場所や接続先を管理する情報である。トポロジ情報は、位置情報と、接続切断情報とを用いて構成される。位置情報には、例えば、転送ノード２００の識別子と、転送ノード２００のコネクタの識別子と、それらが設置された場所との組を含む。

[0068] <接続切断情報>

転送ノード２００Ａに対して他の転送ノード２００Ｂ、２００Ｃや様々なホスト１００Ａやネットワーク資源６００Ａを接続・切断した場合には、転送ノード２００Ａは、制御装置３００に対して、「接続切断情報」を通知す

る。接続切断情報は、例えば、転送ノード200Aの識別子と、機器が接続・切断された転送ノード200Aのコネクタの識別子と、接続・切断された機器のMACアドレスと、接続・切断された機器のIPアドレスと、機器の接続・切断の別との組を含む。したがって、ホスト100Aに関する接続切断情報は、ホスト管理情報と、ホスト100Aの接続・切断の別との組を含む。

[0069] 制御装置300は、接続切断情報の通知を受けると、通知された内容を集積し、転送ノード200A～200C同士の接続関係や、転送ノード200Aの先に接続されたホスト100Aやネットワーク資源600Aへ到達するための経路の計算に利用する。

[0070] 制御装置300は、位置情報として持っている転送ノード200A、および、そのコネクタの設置場所の情報と、転送ノード200Aから通知された接続切断情報とを、それらに含まれる転送ノード200Aの識別子や転送ノード200Aのコネクタの識別子を用いて紐付けることで、ホスト100Aやネットワーク資源600Aが接続・切断された場所を特定でき、これらの情報を合わせてトポロジ情報として管理する。

[0071] <トポロジ情報変化通知>

制御装置300は、収集したトポロジ情報の変化、例えば、ホスト100Aやネットワーク資源600Aの接続状態の変化（ネットワーク上における生滅や移動、アドレスの変化等）を、「トポロジ情報変化通知」としてポリシー管理装置320に通知する。ホスト100Aに関するトポロジ情報変化通知は、例えば、ホスト管理情報と、場所と、接続切断の別との組を含む。

[0072] 予め位置情報をポリシー管理装置320と共有することで、トポロジ情報変化通知において、場所の情報を省略することもできる。ポリシー管理装置320は、転送ノード200Aの識別子や、転送ノード200Aのコネクタの識別子を用いて、位置情報との紐付けを行う。このとき、トポロジ情報変化通知は、接続切断情報と同様に、ホスト管理情報と、接続切断の別との組を含む。

[0073] <アクセス制御ポリシー>

ポリシー管理装置 320 は、アクセス制御ポリシー記憶部 321 に格納された「アクセス制御ポリシー」を管理する。アクセス制御ポリシーは、アクセス制御内容を抽象的に記述した情報であり、ポリシー管理装置 320 から制御装置 300 に受け渡される ACL 情報を生成する基となる。

[0074] アクセス制御ポリシーは、アクセス元やアクセス先の指定を組み合わせ、人にとって分かりやすい抽象的な指定によって、アクセス制御内容を記述する。アクセス制御ポリシーは、アクセス元・アクセス先として、例えば、ホスト 100A のアドレスを指定できる。

[0075] また、アクセス制御ポリシーは、アクセス元・アクセス先として、例えば、ホスト 100A を使用しているユーザを指定できる。アクセス制御ポリシーは、アクセス元・アクセス先として、例えば、ホスト 100A を使用しているユーザに関し、認証装置 310A の持つユーザに関する情報を用いて指定できる。例えば、所属が「総務部」であること、勤務地が「拠点 1」であること、権限階層が「課長」であること、担当プロジェクトが「プロジェクト 1」であること、等を用いて指定できる。

[0076] これらのユーザに関する情報を用いて、アクセス元・アクセス先を抽象的・間接的に指定することで、将来、ユーザの持つこれらの情報に変化があり、対象となるべき適切なユーザが増減・変化した場合でも、管理者等がアクセス制御の修正のためにポリシーを度々更新する必要がなくなる。

[0077] 例えば、所属を用いてアクセス元・アクセス先を指定したポリシーについては、ユーザの所属に異動があった場合、ポリシーを更新しなくとも、現在その所属に対応する適切なユーザを導出し、それらのユーザの使用しているホスト 100A を導出し、それらホスト 100A に関するアクセス制御として ACL 情報が再生成され、制御装置 300 のアクセス制御ルールが更新される。

[0078] さらに、アクセス制御ポリシーは、アクセス元・アクセス先として、例えば、ホスト 100A やネットワーク資源 600A を設置している場所を用い

て指定できる。

[0079] 例えば、アクセス元・アクセス先として、「会議室１に設置されているホスト／ネットワーク資源」、「ビル１に設置されているホスト／ネットワーク資源」、「２階フロアに設置されているホスト／ネットワーク資源」、「会社１に設置されているホスト／ネットワーク資源」等の指定ができる。

[0080] ここで、アクセス元・アクセス先にあたるホスト１００やネットワーク資源６００の設置場所が特定できるのは、制御装置３００がトポロジ情報を収集して、ポリシー管理装置３２０に通知しているからである。

[0081] 場所を用いて、アクセス元・アクセス先を抽象的・間接的に指定することで、将来、ホスト１００Ａやネットワーク資源６００Ａの場所に变化があり、対象となるべき適切なホスト１００Ａやネットワーク資源６００Ａが増減・变化した場合でも、管理者等がアクセス制御の修正のためにポリシーを度々更新する必要がなくなる。

[0082] 例えば、場所を用いてアクセス元・アクセス先を指定したポリシーについては、ホスト１００Ａやネットワーク資源６００Ａの場所に变化があった場合、ポリシーを更新しなくとも、現在その場所に対応する適切なホスト１００Ａやネットワーク資源６００Ａを導出し、それらホスト１００Ａやネットワーク資源６００Ａに関するアクセス制御としてＡＣＬ情報が再生成され、制御装置３００のアクセス制御ルールが更新される。

[0083] また、アクセス制御ポリシーは、アクセス元・アクセス先として、例えば、ホスト１００Ａを使用しているユーザと場所の両方を複合的に用いて指定できる。

[0084] 例えば、アクセス元・アクセス先として、「ユーザ１が居る部屋に設置されているホスト／ネットワーク資源」や、「監査部門のユーザが居る部屋に設置されているホスト／ネットワーク資源」、「責任者のユーザと一緒に居る（同じ場所に居る）ユーザのホスト／ネットワーク資源」等の指定ができる。

[0085] ここで、ユーザの場所が特定できるのは、ユーザの使用しているホスト１

00を、転送ノード200に接続し、認証装置310によって認証することによって、そのホスト100に関する接続切断情報によってホスト100の場所が判明し、認証情報によってホスト100の使用ユーザが判明し、これを紐付けることが可能であるからである。

[0086] 他に、会議予約システム等と連携し、会議に必要なアクセス制御を簡単に指定できるように、管理者や個々のユーザは、アクセス許可の範囲についていくつかのテンプレート（例えば、参加者間アクセス許可）を与えて選択するだけで、ポリシー管理装置320が会議予約システムから自動的に当該会議情報を読み取って「当該会議時間、当該会議室にある当該会議参加ユーザのホストやネットワーク資源」間のみアクセスを許可するアクセス制御ポリシーを適用するような使い方も考えられる。

[0087] <リソース情報>

ポリシー管理装置320は、リソース情報記憶部322に記録された「リソース情報」を管理する。リソース情報は、ホスト100Aやネットワーク資源600Aの情報である。ポリシー管理装置320は、アクセス制御ポリシーからACL情報を生成する際に、リソース情報を参照する。リソース情報は、例えば、ホスト100やネットワーク資源600のMACアドレスとIPアドレスとの組を含む。

[0088] <認証情報紐付け手段>

認証情報紐付け手段323は、認証情報の紐付けを行う。つまり、リソース情報に含まれるMACアドレスと、認証情報に含まれるMACアドレスとをつきあわせることで、1つのレコードとしてまとめて参照できる。これによって、認証情報に含まれるユーザIDをリソース情報と紐付けて利用することができるため、アクセス制御ポリシーにおいて、ユーザIDを用いた抽象的なアクセス元・アクセス先の指定ができ、そのようなアクセス制御ポリシーからACL情報を生成することができる。

[0089] <トポロジ情報紐付け手段>

トポロジ情報紐付け手段324は、トポロジ情報変化通知の紐付けを行う

。つまり、リソース情報に含まれるMACアドレスと、トポロジ情報変化通知に含まれるMACアドレスとをつきあわせることで、1つのレコードとしてまとめて参照できる。これによって、トポロジ情報変化通知に含まれる場所の情報をリソース情報と紐付けて利用することができるため、アクセス制御ポリシーにおいて、場所を用いた抽象的なアクセス元・アクセス先の指定ができ、そのようなアクセス制御ポリシーからACL情報を生成することができる。

[0090] さらに、上記双方の紐付けの結果、認証情報に含まれるユーザIDと、トポロジ情報変化通知に含まれる場所の情報を紐付けて利用することができるため、アクセス制御ポリシーにおいて、ユーザIDおよび、それに付随する情報と場所の情報の両方を複合的に用いた抽象的なアクセス元・アクセス先の指定ができ、そのようなアクセス制御ポリシーからACL情報を生成することができる。

[0091] <アクセス制御リスト（ACL）情報>

ポリシー管理装置320は、「ACL情報」を制御装置300に受け渡す。ACL情報は、アクセス制御内容を記述した情報であり、アクセス制御ポリシーから導出される。ACL情報は、例えば、送信元ホスト100のMACアドレスとIPアドレスとの組、送信先ネットワーク資源600のMACアドレスとIPアドレスとの組、送信元と送信先の通信内容や方向とその可否、とを含む。

[0092] <アクセス制御ルール>

制御装置300は、「アクセス制御ルール」を参照して、フローの通信可否を判定する。アクセス制御ルールは、フローを定義する、送信元のホスト管理情報と、送信先（ネットワーク資源600）のホスト管理情報と、その間の通信内容や方向に対して、可否を定義する。

[0093] <経路>

制御装置300は、複数の転送ノード200Aが接続されたネットワークにおける「経路」を算出する。経路は、フローの送信元ホスト100から送

信先ネットワーク資源 600 に到達する間に経由する転送ノード 200A の辿り方を示す。

[0094] <処理規則>

制御装置 300 は、「処理規則」を転送ノード 200 に受け渡す。処理規則は、転送ノード 200A が、あるフローのパケットを受け取ったときに、それをどのように処理するかを定義する。

[0095] <処理規則設定要求>

転送ノード 200A は、「処理規則設定要求」を制御装置 300 に受け渡す。処理規則設定要求は、転送ノード 200A に到達した未認証パケットの処理を定義する処理規則を、制御装置 300 に対して要求するために使用される。転送ノード 200A は、例えば、パケットを受け取った転送ノード 200A およびコネクタの識別子と、パケットのヘッダ情報を切り出したものと、処理規則設定要求に含める。

[0096] 以下では、本実施形態の通信システムの構成および動作について、図面を参照しつつ、さらに詳細に説明する。ここでは、一例として、会議室群におけるホスト 100A、認証装置 310A、転送ノード 200A、ネットワーク資源 600A について説明するが、居室群およびサーバプールについても、同様である。

[0097] ホスト 100A は、認証装置 310A に対してパケットを送出し、認証装置 310A からの応答に基づき、自身に対する認証手続きを受ける。認証済みのホスト 100A は、ネットワーク資源 600A を利用するためにアクセスパケットを送出し、ネットワーク資源 600A からの応答に基づき、ネットワーク資源 600A との通信を開始する。

[0098] 認証装置 310A は、ホスト 100A からの要求を受けて、ホスト 100A およびユーザの認証を行う。認証装置 310A は、認証済みとなったホスト 100A およびユーザの情報について、認証情報変化通知として、ポリシー管理装置 320 に受け渡す。

[0099] ネットワーク資源 600A は、ホスト 100A からの要求を受けて、サー

ビス利用のための通信を開始する。

[0100] 転送ノード200Aは、ホスト100Aと認証装置310Aとネットワーク資源600Aが送出したパケットを取得し、制御装置300に処理規則設定要求を行う。転送ノード200Aは、制御装置300から受け渡された処理規則に従って、ホスト100Aと認証装置310Aとネットワーク資源600Aが送出したパケットの処理を行う。

[0101] 制御装置300は、転送ノード200Aから受け渡された処理規則設定要求について、要求に記載されたパケットの情報が、ホスト100Aがネットワーク資源600Aにアクセスするパケットであれば、アクセス制御ルールの確認と経路計算を行い、許可すべきフローの場合には、ホスト100Aからネットワーク資源600Aへの当該パケットによる通信を許可する処理規則を生成し、転送ノード200Aに受け渡す。制御装置300は、転送ノード200Aから受け渡された接続切断情報について、これを収集し、経路計算の材料としてトポロジ情報記憶部301に格納するとともに、トポロジ情報変化通知を生成してポリシー管理装置320に受け渡す。

[0102] ポリシー管理装置320は、トポロジ情報紐付け手段324および認証情報紐付け手段323を備えている。

[0103] トポロジ情報紐付け手段324は、制御装置300から受け渡されたトポロジ情報変化通知について、変化のあったトポロジ情報に含まれるMACアドレスと一致するものを、リソース情報記憶部322の既存のリソース情報に含まれるMACアドレスの中から探し、存在する場合には、当該リソース情報を変化のあったトポロジ情報で更新する。一方、一致するものが存在しない場合には、トポロジ情報紐付け手段324は、新たなリソース情報としてリソース情報記憶部322に追加する。また、トポロジ情報紐付け手段324は、トポロジ情報に含まれる位置情報の紐付けを行い、使用中のアクセス制御ポリシーにおいて使用中のリソースである場合には、使用中のアクセス制御ポリシーのリソース指定において使用されている場所のリソースとアクセス制御ポリシー記憶部321のアクセス制御ポリシーに基づいてACL

情報を生成し、制御装置 300 に受け渡す。

[0104] 一方、認証情報紐付け手段 323 は、認証装置 310A から受け渡された認証情報変化通知について、通知に記載された認証情報を用いてリソース情報記憶部 322 に対する更新を行う。使用中のアクセス制御ポリシーのリソース指定において使用されているリソースと一致する場合や、更新対象となったリソースと紐付くユーザ ID が、その時点でアクセス制御ポリシーのリソース指定において使用されているユーザ ID と一致する場合には、認証情報紐付け手段 323 は、アクセス制御ポリシー記憶部 321 のアクセス制御ポリシーに基づいて ACL 情報を生成し、制御装置 300 に受け渡す。

[0105] 本実施形態の通信システムの動作について、図面を参照して説明する。図 2 は、通信システム（図 1）の動作を一例として示すシーケンス図である。ここでは、一例として、会議室群において、ホスト 100A が接続され、ネットワーク資源 600A との通信を開始するまでの処理について説明する。

[0106] まず、ホスト 100A は、ネットワーク接続を行うため、自身を転送ノード 200A に接続する（ステップ S1）。

[0107] 次に、転送ノード 200A は、接続されたホスト 100A について、接続切断情報を作成し、制御装置 300 に受け渡す（ステップ S2）。また、制御装置 300 は、接続切断情報を読み取り、トポロジ情報記憶部 301 に格納されているトポロジ情報を更新する（ステップ S3）。さらに、制御装置 300 は、トポロジ情報変化通知を作成し、ポリシー管理装置 320 に受け渡す（ステップ S4）。

[0108] 次に、トポロジ情報紐付け手段 324 は、トポロジ情報変化通知を読み取り、リソース情報記憶部 322 に格納されている既存のリソース情報との間で、双方に含まれる MAC アドレスを比較する。同一の MAC アドレスが存在する場合には、トポロジ情報紐付け手段 324 は、既存のリソース情報の内容（例えば、IP アドレス）をトポロジ変化通知の内容で更新する（ステップ S5）。一方、該当するリソース情報が無い場合には、トポロジ情報紐付け手段 324 は、新規のホスト管理情報として、リソース情報をリソース

情報記憶部 322 に追加する。また、トポロジ情報紐付け手段 324 は、トポロジ情報変化通知を読み取り、リソース情報記憶部 322 に格納されているリソース情報との間で、双方に含まれるアドレス情報、例えば、MAC アドレスを比較し、同一の MAC アドレスのリソース情報と、トポロジ情報変化通知との間で紐付けを行う（ステップ S6）。この紐付けにより、リソース情報に対し、転送ノードの識別子、転送ノードのコネクタの識別子、場所の情報について、紐付けて参照できるようになる。

[0109] 次に、ホスト 100A は、ホスト 100A およびユーザの認証を行うため、認証装置 310A に対して認証手続を要求する（ステップ S7）。

[0110] 次に、認証装置 310A は、認証手続を要求したホスト 100A について、ホスト 100A およびユーザの認証手続を行う（ステップ S8）。認証手続によって、ホスト 100A のアドレス情報と、ホスト 100A を使用しているユーザの情報とが組となる。また、システムによっては、認証手続において、ホスト 100A のアドレス情報、例えば IP アドレスが、変更または追加される場合もある。また、認証装置 310A は、認証手続によって新たに得られた情報を、認証情報変化通知として、ポリシー管理装置 320 に受け渡す（ステップ S9）。

[0111] 次に、認証情報紐付け手段 323 は、認証情報変化通知を読み取り、リソース情報記憶部 322 に格納されているリソース情報との間で、双方に含まれるアドレス情報、例えば MAC アドレスを比較し、同一の MAC アドレスのリソース情報と、認証情報変化通知との間で紐付けを行うステップ（ステップ S10）。この紐付けにより、リソース情報に対し、ユーザの情報、例えばユーザ ID について、紐付けて参照できるようになる。

[0112] 次に、ポリシー管理装置 320 は、新たに紐付けや更新の行われたリソース情報について、それら変化した内容が、アクセス制御ポリシーに記載された、アクセス元（サブジェクト）、アクセス先（リソース）の指定に関する変化か否かを、適用済み（ACL 情報の生成および制御装置 300 に受け渡し済み）のアクセス制御ポリシーの指定内容と比較することで導出する（ス

テップS 1 1)。例えば、リソース情報に紐付けられた認証情報に、あるユーザIDが含まれており、当該ユーザIDを用いて、そのユーザIDのホストをアクセス制御ポリシーのリソースとして指定している場合には、ポリシー管理装置320は、このアクセス制御ポリシーに関する変化であると判定する。なお、ステップS 1 1は、ステップS 6の後に行ってもよいし、両方で行ってもよい。

[0113] ステップS 1 1において、紐付けや更新の行われたリソース情報に関する、適用済みのアクセス制御ポリシーが見つかった場合には、ポリシー管理装置320は、これらのアクセス制御ポリシーに基づいて、ACL情報を再生成する（ステップS 1 2）。これにより、アクセス制御ポリシー自体を更新することなく、アクセス制御内容を自動的に適切な内容に更新する。一方、ステップS 1 1において、対象となるアクセス制御ポリシーが見つからなかった場合には、ポリシー管理装置320は、ACL情報の再生成は行わずに、終了する。その後、リソース情報に対する、さらに新たな紐付けや更新が発生し、ステップS 1 1が再度行われた場合は、その際の判定結果に従う。ポリシー管理装置320は、生成したACL情報を、制御装置300に受け渡す（ステップS 1 3）。

[0114] 次に、制御装置300は、受け渡されたACL情報に基づいて、アクセス制御ルールを更新し、経路計算を行って、処理規則を作成する（ステップS 1 4）。なお、制御装置300は、この段階ではアクセス制御ルールの更新のみ行い、転送ノード200Aから処理規則設定要求を受け取った後に、経路計算および処理規則作成を行うようにしてもよい。制御装置300は、作成した処理規則を、転送ノード200Aに受け渡す（ステップS 1 5）。

[0115] これにより、転送ノード200Aは、アクセス制御ポリシーに記載されたアクセス制御を、新たな紐付け・更新が行われたリソース情報に合致した内容で設定された状態となる。

[0116] 次に、ホスト100Aは、転送ノード200Aによるアクセス制御を介して、ネットワーク資源600Aとの通信を行う（ステップS 1 6）。ここで

、ネットワーク資源600Aには、ホスト100A自身およびホスト100A以外のホストも含まれ得る。

[0117] なお、ポリシー管理装置320と、制御装置300と、転送ノード200A～200Cとは、図1に示すように、それぞれ別個のコンピュータシステムで構築されていてもよいし、一部または全部が同一のコンピュータシステムで実現されていてもよい。

[0118] ホスト100A～100Cは、プログラムに従って動作する情報処理装置のCPUと、RAM等の記憶媒体と、認証装置310とネットワーク資源600と通信を行うための通信インタフェースによって実現し得る。

[0119] 同様に、認証装置310A～310Cとネットワーク資源600A～600Cは、プログラムに従って動作する情報処理装置のCPUと、RAM等の記憶媒体と、ホスト100A～100Cと通信を行うための通信インタフェースによって実現し得る。

[0120] また、転送ノード200A～200Cは、プログラムに従って動作する情報処理装置のCPUと、RAM等の記憶媒体と、制御装置300と通信を行うための通信インタフェースと、ホスト100A～100Cと認証装置310A～310Cとネットワーク資源600A～600Cとの間の通信内容を取得するための通信インタフェースによって実現し得る。

[0121] さらに、制御装置300は、プログラムに従って動作する情報処理装置のCPUと、RAM等の記憶媒体と、ポリシー管理装置320と転送ノード200A～200Cと通信を行うための通信インタフェースによって実現し得る。

[0122] また、ポリシー管理装置320は、プログラムに従って動作する情報処理装置のCPUと、RAM等の記憶媒体と、制御装置300と通信を行うための通信インタフェースと、制御装置310A～310Cと通信を行うための通信インタフェースと、RAMやハードディスク等の記憶媒体によって実現し得る。

[0123] 以上説明したように、本実形態に係る通信システムは、

処理対象パケットを特定するための照合規則と該照合規則に適合するパケットに適用する処理内容とを対応付けた処理規則に従って受信パケットを処理し、自身と、自身に接続されたホストの識別子の組を制御装置に送信する複数の転送ノードと、

ホストに対し使用者であるユーザの認証を行い、認証手続で得たホストとユーザの識別子の組をポリシー管理装置に送信する認証装置と、

前記転送ノードから得た転送ノードに接続されたホストの情報をポリシー管理装置に送信し、ポリシー管理装置から得られたホストに関するアクセス制御リストの記述から前記処理規則を設定する制御装置と、

アクセス制御対象のホストの識別子と、ホストが接続された転送ノードの識別子とを紐付けるトポロジ情報紐付け手段と、

アクセス制御対象のホストの識別子と、ホストを使用しているユーザの識別子とを紐付ける認証情報紐付け手段とを有し、

少なくともユーザの識別子または転送ノードの識別子を用いた記載によってアクセス制御対象のホストを特定するアクセス制御ポリシーから、前記アクセス制御リストを生成して制御装置に送信するポリシー管理装置と、を備えている。

[0124] すなわち、本実施形態に係る通信システムは、

フローを特定するための照合規則と該照合規則に適合するパケットに適用する処理内容とを対応付けた処理規則に従って受信パケットを処理し、受信パケットによって検出されたホストおよびネットワーク資源の接続または切断情報をそれらホストおよびネットワーク資源のアドレス情報を伴って制御装置に通知する複数の転送ノードと、

転送ノードに接続されたホストやホストの使用者であるユーザを認証する認証装置と、

前記認証に成功したホストおよびネットワーク資源について検出された接続または切断情報をトリガおよび情報源として、アクセス権限に関する情報を生成して制御装置に提供するポリシー管理装置と、

転送ノードから収集されたホストおよびネットワーク資源に関する接続または切断情報を前記ポリシー管理装置に通知するとともに、前記ポリシー管理装置から受信したアクセス権限に関する情報に基づいて、前記認証に成功したホストと前記ホストがアクセス可能な資源との間の経路を生成し、該経路上の転送ノードに処理規則を設定する制御装置と、を備えている。

[0125] かかる通信システムによると、全く別の機能として存在する、ホストやネットワーク資源等の機器に関するネットワーク制御に必要な管理機能と、ユーザの識別に必要な管理機能とを、簡便かつ自然に繋ぐ方法を提供することができる。したがって、機器が大量に存在し接続状態が頻繁に変化する場合や、ユーザが大量に存在し接続状態が頻繁に変化する場合においても、それら別用途の管理機能そのものを、ポリシーから生成されるACL情報の更新のトリガとして利用するとともに更新すべき情報の取得元として利用することで、両者を繋いで新たなアクセス元・アクセス先の指定方法を提供し、管理者や個々のユーザがアクセス制御ポリシーを多大な手間をかけて更新することなく、リアルタイムにアクセス制御を更新することが可能となる。

[0126] また、本発明によれば、企業等のシステムにおけるネットワークアクセス制御において、各ユーザが、拠点等の間を自由に行き来し、用途・目的に応じて自由に、大量のユーザ、大量の機器を対象とし、頻繁に変化するアクセス制御範囲に追従したアクセス制御を行う場合に、管理者や各ユーザに多大な手間をかけることなく、抽象的なアクセス元・アクセス先の指定が可能なアクセス制御ポリシーを記載するだけで、適切なアクセス制御が実施できるシステムを構築することができる。

[0127] なお、上記の特許文献等の先行技術文献の各開示を、本書に引用をもって繰り込むものとする。本発明の全開示（請求の範囲を含む）の枠内において、さらにその基本的技術思想に基づいて、実施形態の変更・調整が可能である。また、本発明の請求の範囲の枠内において種々の開示要素（各請求項の各要素、各実施形態の各要素、各図面の各要素等を含む）の多様な組み合わせ、ないし、選択が可能である。すなわち、本発明は、請求の範囲を含む全

開示、技術的思想にしたがって当業者であればなし得るであろう各種変形、修正を含むことは勿論である。特に、本書に記載した数値範囲については、当該範囲内に含まれる任意の数値ないし小範囲が、別段の記載のない場合でも具体的に記載されているものと解釈されるべきである。

符号の説明

[0128]	100、100A～100C	ホスト
200、200A～200C	転送ノード	
300	制御装置	
301	トポロジ情報記憶部	
310、310A～310C	認証装置	
320	ポリシー管理装置	
321	アクセス制御ポリシー記憶部	
322	リソース情報記憶部	
323	認証情報紐付け手段	
324	トポロジ情報紐付け手段	
600、600A～600C	ネットワーク資源	

請求の範囲

[請求項1]

処理規則に従ってパケットを処理する複数の転送ノードと、
前記複数の転送ノードを制御する制御装置と、
前記複数の転送ノードのいずれかに接続されたホストを使用するユーザを認証する認証装置と、

アクセス制御対象のホストの識別子とホストが接続された転送ノードの識別子とを紐付ける第1の紐付け手段、および／または、アクセス制御対象のホストの識別子とホストを使用するユーザの識別子とを紐付ける第2の紐付け手段を有し、転送ノードの識別子、および／または、ユーザの識別子を用いてアクセス制御対象のホストを特定するアクセス制御ポリシーを保持するポリシー管理装置と、を備え、

前記複数の転送ノードは、それぞれ、自身に接続されたホストの識別子と自身の識別子との組を前記ポリシー管理装置に送信し、

前記認証装置は、前記複数の転送ノードのいずれかに接続されたホストの識別子とユーザの識別子との組を前記ポリシー管理装置に送信し、

前記ポリシー管理装置は、前記アクセス制御ポリシーを参照し、前記複数の転送ノードにいずれかに接続されたホストがアクセス制御対象である場合には、アクセス制御の内容をアクセス制御リストとして前記制御装置に通知し、

前記制御装置は、前記アクセス制御リストに応じて前記処理規則を生成して、前記複数の転送ノードに設定する、通信システム。

[請求項2]

前記処理規則は、処理対象パケットを特定するための照合規則と、該照合規則に適合するパケットに適用する処理内容とを対応付けたものである、請求項1に記載の通信システム。

[請求項3]

前記複数の転送ノードは、それぞれ、自身に接続されたホストの識別子と自身の識別子との組を、前記制御装置を経由して前記ポリシー管理装置に送信する、請求項1または2に記載の通信システム。

- [請求項4] 前記制御装置は、前記複数の転送ノードのいずれかに接続されたホストの識別子と該転送ノードの識別子との組をトポロジ情報として保持し、前記アクセス制御リストに応じたパケットの処理規則を該トポロジ情報に基づいて生成する、請求項3に記載の通信システム。
- [請求項5] 前記アクセス制御ポリシーは、アクセス制御対象のホストを特定するために、所定の場所に設置された転送ノードの識別子のリストを含む、請求項1ないし4のいずれか1項に記載の通信システム。
- [請求項6] 前記アクセス制御ポリシーは、アクセス制御対象のホストを特定するために、所定の所属、所定の勤務地、所定の権限階層、および、所定の担当プロジェクトのうちの少なくともいずれかに該当するユーザの識別子のリストを含む、請求項1ないし4のいずれか1項に記載の通信システム。
- [請求項7] 処理規則に従ってパケットを処理する複数の転送ノードと、アクセス制御リストに応じて該処理規則を生成して該複数の転送ノードに設定する制御装置と、該複数の転送ノードのいずれかに接続されたホストを使用するユーザを認証する認証装置と、を備えた通信システムにおけるポリシー管理装置であって、
- アクセス制御対象のホストの識別子とホストが接続された転送ノードの識別子とを紐付ける第1の紐付け手段、および／または、アクセス制御対象のホストの識別子とホストを使用するユーザの識別子とを紐付ける第2の紐付け手段と、
- 転送ノードの識別子、および／または、ユーザの識別子を用いてアクセス制御対象のホストを特定するアクセス制御ポリシーを保持するアクセス制御ポリシー記憶部と、を備え、
- 前記複数の転送ノードのそれぞれから、自身に接続されたホストの識別子と自身の識別子との組を受信し、
- 前記複数の転送ノードのいずれかに接続されたホストの識別子とユーザの識別子との組を前記認証装置から受信し、

前記アクセス制御ポリシーを参照し、前記複数の転送ノードにいずれかに接続されたホストがアクセス制御対象である場合には、アクセス制御の内容を前記アクセス制御リストとして前記制御装置に通知する、ポリシー管理装置。

[請求項8]

複数の転送ノードと、該複数の転送ノードを制御する制御装置と、該複数の転送ノードのいずれかに接続されたホストを使用するユーザを認証する認証装置と、転送ノードの識別子、および／または、ユーザの識別子を用いてアクセス制御対象のホストを特定するアクセス制御ポリシーを保持するポリシー管理装置と、を備えた通信システムにおける通信方法であって、

前記複数の転送ノードが、それぞれ、自身に接続されたホストの識別子と自身の識別子との組を前記ポリシー管理装置に送信する工程と、

前記認証装置が、前記複数の転送ノードのいずれかに接続されたホストの識別子とユーザの識別子との組を前記ポリシー管理装置に送信する工程と、

前記ポリシー管理装置が、アクセス制御対象のホストの識別子とホストが接続された転送ノードの識別子とを紐付ける工程、および／または、

アクセス制御対象のホストの識別子とホストを使用するユーザの識別子とを紐付ける工程と、

前記アクセス制御ポリシーを参照し、前記複数の転送ノードにいずれかに接続されたホストがアクセス制御対象である場合には、アクセス制御の内容をアクセス制御リストとして前記制御装置に通知する工程と、

前記制御装置が、前記アクセス制御リストに応じてパケットの処理規則を生成して、前記複数の転送ノードに設定する工程と、

前記複数の転送ノードが前記処理規則に従ってパケットを処理する

工程と、を含む、通信方法。

[請求項9] 前記処理規則は、処理対象パケットを特定するための照合規則と、該照合規則に適合するパケットに適用する処理内容とを対応付けたものである、請求項8に記載の通信方法。

[請求項10] 前記複数の転送ノードは、それぞれ、自身に接続されたホストの識別子と自身の識別子との組を、前記制御装置を経由して前記ポリシー管理装置に送信する、請求項8または9に記載の通信方法。

[請求項11] 前記制御装置は、前記複数の転送ノードのいずれかに接続されたホストの識別子と該転送ノードの識別子との組をトポロジ情報として保持し、前記アクセス制御リストに応じたパケットの処理規則を該トポロジ情報に基づいて生成する、請求項10に記載の通信方法。

[請求項12] 前記アクセス制御ポリシーは、アクセス制御対象のホストを特定するために、所定の場所に設置された転送ノードの識別子のリストを含む、請求項8ないし11のいずれか1項に記載の通信方法。

[請求項13] 前記アクセス制御ポリシーは、アクセス制御対象のホストを特定するために、所定の所属、所定の勤務地、所定の権限階層、および、所定の担当プロジェクトのうちの少なくともいずれかに該当するユーザの識別子のリストを含む、請求項8ないし11のいずれか1項に記載の通信方法。

[請求項14] 処理規則に従ってパケットを処理する複数の転送ノードと、アクセス制御リストに応じて該処理規則を生成して該複数の転送ノードに設定する制御装置と、該複数の転送ノードのいずれかに接続されたホストを使用するユーザを認証する認証装置と、を備えた通信システムにおいて、転送ノードの識別子、および／または、ユーザの識別子を用いてアクセス制御対象のホストを特定するアクセス制御ポリシーを保持するポリシー管理装置が、

アクセス制御対象のホストの識別子とホストが接続された転送ノードの識別子とを紐付ける工程、および／または、

アクセス制御対象のホストの識別子とホストを使用するユーザの識別子とを紐付ける工程と、

前記複数の転送ノードのそれぞれから、自身に接続されたホストの識別子と自身の識別子との組を受信する工程と、

前記複数の転送ノードのいずれかに接続されたホストの識別子とユーザの識別子との組を前記認証装置から受信する工程と、

前記アクセス制御ポリシーを参照し、前記複数の転送ノードにいずれかに接続されたホストがアクセス制御対象である場合には、アクセス制御の内容を前記アクセス制御リストとして前記制御装置に通知する工程と、を含む、通信方法。

[請求項15]

処理規則に従ってパケットを処理する複数の転送ノードと、アクセス制御リストに応じて該処理規則を生成して該複数の転送ノードに設定する制御装置と、該複数の転送ノードのいずれかに接続されたホストを使用するユーザを認証する認証装置と、を備えた通信システムにおいて、転送ノードの識別子、および／または、ユーザの識別子を用いてアクセス制御対象のホストを特定するアクセス制御ポリシーを保持するポリシー管理装置に設けられたコンピュータに対して、

アクセス制御対象のホストの識別子とホストが接続された転送ノードの識別子とを紐付ける処理、および／または、

アクセス制御対象のホストの識別子とホストを使用するユーザの識別子とを紐付ける処理と、

前記複数の転送ノードのそれぞれから、自身に接続されたホストの識別子と自身の識別子との組を受信する処理と、

前記複数の転送ノードのいずれかに接続されたホストの識別子とユーザの識別子との組を前記認証装置から受信する処理と、

前記アクセス制御ポリシーを参照し、前記複数の転送ノードにいずれかに接続されたホストがアクセス制御対象である場合には、アクセス制御の内容を前記アクセス制御リストとして前記制御装置に通知す

る処理と、を実行させる、プログラム。