

【公報種別】特許法第17条の2の規定による補正の掲載  
 【部門区分】第7部門第3区分  
 【発行日】平成20年3月21日(2008.3.21)

【公表番号】特表2005-537687(P2005-537687A)  
 【公表日】平成17年12月8日(2005.12.8)  
 【年通号数】公開・登録公報2005-048  
 【出願番号】特願2003-531370(P2003-531370)  
 【国際特許分類】

H 0 4 L 12/56 (2006.01)  
 G 0 6 F 9/46 (2006.01)  
 G 0 6 F 12/00 (2006.01)  
 G 0 6 F 15/177 (2006.01)

【 F I 】

H 0 4 L 12/56 B  
 H 0 4 L 12/56 2 0 0 Z  
 G 0 6 F 9/46 3 6 0 B  
 G 0 6 F 12/00 5 4 5 A  
 G 0 6 F 15/177 6 7 4 A  
 G 0 6 F 15/177 6 7 8 A

【誤訳訂正書】  
 【提出日】平成20年1月17日(2008.1.17)  
 【誤訳訂正1】  
 【訂正対象書類名】特許請求の範囲  
 【訂正対象項目名】全文  
 【訂正方法】変更  
 【訂正の内容】  
 【特許請求の範囲】  
 【請求項1】

コンテンツプロバイダのリソースが少なくとも2つの異なるネットワークからクライアントへ配信されるインターネットコンテンツの配信用フレームワークであって、

加入者サーバネットワークと、

前記加入者サーバネットワークとは異なる少なくとも1つのコンテンツ配信ネットワーク(CDN)と、

ポリシーに基づいてドメインネームサービスを提供する少なくとも1つのドメインネームサーバと

を備え、

ホスト名の解決を求めるクライアントの要求に応じて、前記ドメインネームサーバは、少なくとも1つのポリシーに対する考慮に少なくとも部分的に基づいて、(a)前記少なくとも1つのコンテンツ配信ネットワークと(b)前記加入者サーバネットワークとのいずれか1つを選択し、前記ドメインネームサーバは前記選択されたネットワークに関連する情報を前記クライアントに提供する、フレームワーク。

【請求項2】

ホスト名の解決を求める要求に応じて、前記ドメインネームサーバは、少なくとも前記クライアントの所在位置および別のポリシーに対する考慮の少なくとも一部に基づいて、1つのネットワークを選択する請求項1記載のフレームワーク。

【請求項3】

前記ドメインネームサーバは、  
 (a)地理的ポリシーと、

(b) 負荷共有ポリシーと、  
(c) オーバーフローポリシーと、  
(d) ネットワークを意識したポリシーとのうちの1以上に基づいて1つのネットワークを選択する請求項1記載のフレームワーク。

【請求項4】

前記少なくとも1つのポリシーに対する考慮は、  
要求元クライアントの地理上の所在位置に基づいて1つのネットワークの選択を決定する地政学に関するポリシーと、

前記加入者サーバネットワークと前記少なくとも1つのコンテンツ配信ネットワーク(CDN)とに関連する動的負荷情報に基づいて1つのネットワークの選択を決定する負荷共有ポリシーと、

1つのネットワークの負荷を別のネットワークに分散する方法を決定する分散ポリシーと、

前記ネットワーク内の少なくとも1つのサーバが機能しなくなった場合、そのネットワークの選択を決定する部分的フェイルオーバーポリシーと、

前の層内のサーバが機能しなくなった場合、サーバグループに対応するサーバ階層内の次の層のサーバの選択を決定するフェイルオーバーポリシーと、

モニタ対象サーバと管理対象サーバのうちの1つとして前記ネットワーク内のサーバを定義するサーバ指定ポリシーと

のうちの少なくとも1つを含む請求項1記載のフレームワーク。

【請求項5】

ドメインネームサービスを提供するドメインネームサーバであって、

要求者の所在位置を決定する所在位置決定装置と、

ポリシーに基づいてドメインネームサービスを提供する適応型トラフィック制御メカニズムと

を備え、

前記ドメインネームサーバは、

- (a) 地理的ポリシーと、
- (b) 負荷共有ポリシーと、
- (c) オーバーフローポリシーと、
- (d) ネットワークを意識したポリシーと

のうちの1以上のポリシーに少なくとも部分的に基づいて、少なくとも2つの異なるコンテンツ配信ネットワーク(CDN)と加入者サーバネットワークとから1つのサーバネットワークを選択することを試みる、ドメインネームサーバ。

【請求項6】

コンテンツプロバイダのリソースが、加入者サーバネットワークと前記加入者サーバネットワークとは異なる少なくとも1つのコンテンツ配信ネットワーク(CDN)とを含む少なくとも2つの異なるネットワークからクライアントへ配信されるフレームネットワーク内で操作可能な、ドメインネームサービスを提供する方法であって、

ホスト名の解決を求める要求をリゾルバから受信するステップと、

前記要求元リゾルバの所在位置を決定するステップと、

前記決定された所在位置と、別の動的ポリシーに対する考慮とに少なくとも部分的に基づいて、(a)前記少なくとも1つのコンテンツ配信ネットワークと(b)前記加入者サーバネットワークとのいずれか1つを選択するステップと、

前記要求元リゾルバへ前記選択されたネットワークに関連する情報であって、前記選択されたネットワークに関連するドメインネームを含む情報を提供するステップと、  
を備える方法。

【請求項7】

前記ネットワークは、

- (a) 地理的ポリシーと、

- (b) 負荷共有ポリシーと、
- (c) 負荷分散ポリシーと、
- (d) ネットワークを意識したポリシーと

のうちの1以上のポリシーに基づいて選択される請求項6記載の方法。

【請求項8】

インターネットコンテンツの配信用フレームワークであって、  
インターネットコンテンツを提供する加入者に関連するサーバネットワークと、  
前記加入者に関連するサーバネットワークとは異なる少なくとも1つのコンテンツ配信ネットワーク(CDN)と、

ポリシーに基づいてドメインネームサービスを提供する少なくとも1つのドメインネームサーバを備える適応型トラフィック制御(ATC)ネームサーバネットワークと  
を備え、

ホスト名の解決を求める要求に応じて、前記ATCネームサーバネットワーク内の少なくとも1つのドメインネームサーバが、少なくとも1つのポリシーに対する考慮の少なくとも一部に基づいて、(a)前記少なくとも1つのCDNと(b)前記加入者に関連するサーバネットワークとのいずれか1つを選択し、

前記少なくとも1つのドメインネームサーバは、前記選択されたネットワークに関連する情報を要求者に提供し、

前記情報は、(a)前記選択されたネットワークがCDNの場合の前記選択されたネットワークのドメインネームと(b)前記選択されたネットワークが前記加入者に関連するサーバネットワークの場合の前記加入者に関連するサーバネットワーク内のサーバのアドレスとのいずれかを含む、フレームワーク。

【請求項9】

前記ポリシーに対する考慮は、

- (a) 地理的ポリシーに対する考慮と、
- (b) 負荷共有ポリシーに対する考慮と、
- (c) オーバーフローポリシーに対する考慮と、
- (d) ネットワークを意識したポリシーに対する考慮と

のうちの1以上の考慮を備える請求項8記載のフレームワーク。

【請求項10】

適応型トラフィック制御用フレームワークであって、

加入者サーバネットワークと前記加入者サーバネットワークとは異なる少なくとも1つのコンテンツ配信ネットワーク(CDN)とを含む複数の異なるサーバネットワークと、  
適応型ポリシーに基づいてドメインネームサービスを提供する少なくとも1つのドメインネームサーバを備える適応型トラフィック制御(ATC)ネームサーバネットワークと  
を備え、

ホスト名の解決を求める要求に応じて、前記ATCドメインネームサーバネットワーク内の少なくとも1つのドメインネームサーバが、ポリシーと、前記要求者の所在位置とに少なくとも部分的に基づいて、(a)前記少なくとも1つのコンテンツ配信ネットワークと(b)前記加入者サーバネットワークとのいずれか1つを選択し、

前記少なくとも1つのドメインネームサーバは、前記選択されたネットワークに関連する情報を提供する、フレームワーク。

【請求項11】

前記選択されたネットワークに関連する情報は、

前記選択されたネットワークに関連するドメインネームまたはCNAMEを含む請求項10記載のフレームワーク。

【請求項12】

前記加入者サーバネットワークは少なくとも1つのサーバグループを備え、前記少なくとも1つのサーバグループの個々のサーバがサーバ階層に対応する請求項11記載のフレームワーク。

## 【請求項 1 3】

前記サーバ階層は、  
少なくとも1つの一次サーバを備える第1層と、  
前記第1層内の前記少なくとも1つの一次サーバが機能しなくなった場合に機能する少なくとも1つの第1のレベルのオーバーフローサーバを備える第2層と、  
前記少なくとも1つの一次サーバと、前記1以上の第1のレベルのオーバーフローサーバとの双方が機能しなくなった場合、少なくとも1つの第2のレベルのオーバーフローサーバを備える第3層とのうちの少なくとも1つの層を含む請求項1 2記載のフレームワーク。

## 【請求項 1 4】

前記サーバネットワーク内の個々のサーバは、  
モニタ対象サーバと、  
管理対象サーバと  
のうち少なくとも1つであり、  
前記モニタ対象サーバの利用可能性が動的にモニタされ、  
前記管理対象サーバの利用可能性が動的にモニタされるか、または、前記管理対象サーバの負荷共有もしくは分散部分が動的に定義される、請求項1 3記載のフレームワーク。

## 【請求項 1 5】

前記 A T C ドメインネームサーバネットワーク内の個々のドメインネームサーバは、  
要求元クライアントの地理上の所在位置を決定する所在位置決定装置と、  
前記ポリシーベースのドメインネームサービスを容易に行うことが可能な適応型トラフィック制御 ( A T C ) メカニズムと、を備える請求項1 4記載のフレームワーク。

## 【請求項 1 6】

前記少なくとも1つのポリシーは、  
前記クライアントの地理上の位置に基づいて、前記サーバネットワーク内のサーバグループの選択を決定する地政学に関するポリシーと、  
サーバグループ内のサーバと関連する動的負荷共有情報に基づいて、前記サーバグループからのサーバの選択を決定する負荷共有ポリシーと、  
サーバグループ内のサーバの負荷を別のサーバに分散する方法を決定する分散ポリシーと、  
同じ層のサーバのうちの少なくとも1つのサーバが機能しなくなった場合、サーバ階層の層のサーバの選択を決定するフェイルオーバーポリシーと、  
前の層内のサーバが機能しなくなった場合、サーバ階層内の次の層のサーバの選択を決定する層化フェイルオーバーポリシーと、  
モニタ対象サーバと管理対象サーバとのうちの少なくとも1つとして前記サーバネットワーク内のサーバを定義するサーバ指定ポリシーとのうちの少なくとも1つのポリシーを含む請求項1 5記載のフレームワーク。

## 【請求項 1 7】

前記地政学に関するポリシーは、  
大陸ベースのポリシーと、  
国ベースのポリシーと、  
領域ベースのポリシーと、  
時間帯ベースのポリシーと  
のうちの少なくとも1つを含む請求項1 6記載のフレームワーク。

## 【請求項 1 8】

調整ポリシーをさらに備える請求項1 7記載のフレームワーク。

## 【請求項 1 9】

前記ドメインネームサーバは、前記ドメインネームサーバの作動中に生じるイベントを観察することが可能なモニタエージェントをさらに備える請求項1 5記載のフレームワーク。

## 【請求項 20】

前記モニタエージェントは、モニタ対象サーバか、管理対象サーバかのいずれかとして指定される、前記サーバネットワーク内の1以上のサーバの利用可能性がモニタされるようにさらに構成され、それによって、前記ドメインネームサーバは、前記1以上のサーバの利用可能性に基づいて前記サーバを決定することができる請求項19記載のフレームワーク。

## 【請求項 21】

前記モニタエージェントは、1以上の管理対象サーバから動的負荷共有情報と負荷分散情報とのポーリングを行うことが可能であり、それによって前記ドメインネームサーバは、前記管理対象サーバと関連する前記動的負荷共有情報と前記負荷分散情報とに基づいてサーバを決定することができる請求項20記載のフレームワーク。

## 【請求項 22】

前記ATCネームサーバネットワークの作動と、前記サーバネットワークの状態とを管理することが可能な適応型トラフィック制御(ATC)管理フレームワークをさらに備える請求項19記載のフレームワーク。

## 【請求項 23】

前記ATC管理フレームワークは、  
管理マスタエージェント(A MA)と、  
少なくとも1つの管理マスタバックアップエージェントと、  
ネットワークオペレーションセンタと  
を備える請求項22記載のフレームワーク。

## 【請求項 24】

前記A MAは、  
前記少なくとも1つのドメインネームサーバの少なくとも1つのモニタエージェントから受信したイベント情報によって前記ATCドメインネームサーバネットワークの作動をモニタすることが可能なATCネットワークモニタメカニズムと、  
少なくとも1つのソースから少なくとも1つのポリシーを受信し、これを動的にポーリングし、前記ATCドメインネームサーバネットワーク内の前記少なくとも1つのドメインネームサーバへ前記少なくとも1つのポリシーを配信することが可能なATCポリシー管理メカニズムと、  
前記A MAが機能しなくなった場合、前記A MAの代わりに機能できるように、前記少なくとも1つの管理マスタエージェントがバックアップすることを可能にする管理マスタバックアップメカニズムと  
を備える請求項23記載のフレームワーク。

## 【請求項 25】

前記少なくとも1つのソースは、  
加入者ポリシーを定義するべく前記管理マスタエージェントとリアルタイムで交信し、前記ATCポリシー管理メカニズムによってポーリングを行うことが可能な動的ポリシーを提供することが可能な加入者と、  
前記ATCポリシー管理メカニズムが受信または動的ポーリングを行うことが可能なポリシーを定義する1以上のポリシーエンティティと、  
ポーリングを行うことが可能な動的負荷共有ポリシーと負荷分散ポリシーとを提供する前記サーバネットワーク内の1以上の管理対象サーバと  
のうちの少なくとも1つを含む請求項24記載のフレームワーク。

## 【請求項 26】

前記ATCネットワークモニタメカニズムは、  
異なるATCドメインネームサーバと関連するモニタエージェントからイベント情報を受信し、そのトラップしたイベント情報を統合することが可能なトラップハンドラと、  
前記統合されたトラップ済みイベント情報を分析することが可能な処理メカニズムと、  
前記処理から得られた処理結果に基づいて警告を生成し、前記ネットワークオペレーシ

ョンセンタへ前記警告を送信する警告生成メカニズムと、を備える請求項24記載のフレームワーク。

【請求項27】

前記警告生成メカニズムは、前記加入者へ前記警告を送信することがさらに可能である請求項26記載のフレームワーク。

【請求項28】

コンテンツプロバイダのリソースが、加入者サーバネットワークと前記加入者サーバネットワークとは異なる少なくとも1つのコンテンツ配信ネットワーク(CDN)とを含む少なくとも2つの異なるサーバネットワークからクライアントへ配信されるフレームワーク内で操作可能な、ホスト名を解決するドメインネームサーバであって、

ホスト名の解決を求める要求を受信した要求元クライアントの地理上の所在位置を決定することが可能な所在位置決定装置と、

ポリシーベースのドメインネームサービスをサポートすることが可能な適応型トラフィック制御(ATC)メカニズムと

を備え、

前記ドメインネームサーバは、(a)前記少なくとも1つのコンテンツ配信ネットワークと(b)前記加入者サーバネットワークとのいずれか1つを選択して、前記少なくとも2つのネットワークのうちの前記選択された1つと関連する少なくとも1つのドメインネームである回答を提供し、

前記ネットワークの前記選択は、前記所在位置決定装置により確かめられた前記所在位置と、少なくとも1つのポリシーとに少なくとも基づく、ドメインネームサーバ。

【請求項29】

前記少なくとも2つの異なるサーバネットワークは、

少なくとも1つのサーバグループを備える加入者サーバネットワークと、

少なくとも1つのサーバを備えるコンテンツ配信ネットワーク(CDN)と

のうちの少なくとも1つを含む、請求項28記載のドメインネームサーバ。

【請求項30】

個々のサーバグループは、

少なくとも1つの一次サーバを備える第1層と、

前記少なくとも1つの一次サーバが機能しなくなった場合に機能する1以上の第1のレベルのオーバーフローサーバを備える第2層と、

前記少なくとも1つの一次サーバと、前記1以上の第1のレベルのオーバーフローサーバとの双方が機能しなくなった場合、1以上の第2のレベルのオーバーフローサーバを備える第3層と

のうちの少なくとも1つの層を含むサーバ階層に対応する、請求項29記載のドメインネームサーバ。

【請求項31】

前記少なくとも1つのポリシーは、

前記クライアントの地理上の位置に基づいて、サーバネットワークの選択を決定する地政学に関するポリシーと、

前記サーバと関連する動的負荷共有情報に基づいて、サーバネットワークの選択を決定する負荷共有ポリシーと、

サーバネットワークの負荷を別のサーバネットワークに分散する方法を決定する分散ポリシーと

のうちの少なくとも1つを含む、請求項28記載のドメインネームサーバ。

【請求項32】

前記地政学ポリシーは、

大陸ベースのポリシーと、

国ベースのポリシーと、

領域ベースのポリシーと、

時間帯ベースのポリシーと

のうちの少なくとも1つを含む、請求項3 1記載のドメインネームサーバ。

【請求項3 3】

調整ポリシーをさらに備える請求項3 1記載のドメインネームサーバ。

【請求項3 4】

前記ドメインネームサーバの作動中に生じるイベントを観察し、適応型トラフィック制御（A T C）管理フレームワークの適応型トラフィック制御（A T C）ネットワークモニタメカニズムへこのようなイベントを送信することが可能なモニタエージェントをさらに備える請求項2 8記載のドメインネームサーバ。

【請求項3 5】

コンテンツプロバイダのリソースが、加入者サーバネットワークと前記加入者サーバネットワークとは異なる少なくとも1つのコンテンツ配信ネットワーク（C D N）とを含む少なくとも2つの異なるネットワークからクライアントへ配信されるフレームワーク内で操作可能な、適応型トラフィック制御ベースのドメインネームサービスのための方法であって、

適応型トラフィック制御（A T C）ドメインネームサーバネットワーク内のドメインネームサーバにより、ホスト名の解決を求めるリゾルバからの要求を受信するステップと、

前記クライアントの前記地理上の所在位置と、少なくとも1つのポリシーとに少なくとも部分的に基づいて、（a）前記少なくとも1つのコンテンツ配信ネットワークと（b）前記加入者サーバネットワークとのいずれか1つから選択されたサーバネットワークに対応する回答を決定するステップと、

前記回答を要求者へ提供するステップと  
を備え、

前記回答は、前記選択されたサーバネットワークのドメインネームと、前記選択されたサーバネットワークのC N A M Eのうちの少なくとも1つである、方法。

【請求項3 6】

前記少なくとも2つの異なるサーバネットワークは、  
コンテンツ配信サービスを提供する加入者サーバネットワークと、  
前記コンテンツ配信サービスを提供するコンテンツ配信ネットワーク（C D N）と  
のうちの少なくとも1つを含む、請求項3 5記載の方法。

【請求項3 7】

前記加入者サーバネットワークは、少なくとも1つのサーバグループを含む、請求項3 6記載の方法。

【請求項3 8】

個々のサーバグループは、  
少なくとも1つの一次サーバを備える第1層と、

前記少なくとも1つの一次サーバが機能しなくなった場合に機能する1以上の第1のレベルのオーバーフローサーバを備える第2層と、

前記少なくとも1つの一次サーバと、前記1以上の第1のレベルのオーバーフローサーバとの双方が機能しなくなった場合に機能する1以上の第2のレベルのオーバーフローサーバを備える第3層と

のうちの少なくとも1つを含むサーバ階層に対応する、請求項3 7記載の方法。

【請求項3 9】

前記サーバネットワーク内の個々のサーバを、  
モニタ対象サーバと、  
管理対象サーバと

のうちの少なくとも1つのサーバとして指定することができ、

前記モニタ対象サーバの利用可能性が動的にモニタされ、

前記管理対象サーバの利用可能性が動的にモニタされるか、または前記管理対象サーバの負荷共有もしくは負荷分散が動的に定義される、請求項3 8記載の方法。

## 【請求項 4 0】

前記少なくとも 1 つのポリシーは、  
前記クライアントの地理上の位置に基づいて、サーバネットワークの選択を決定する地政学に関するポリシーと、  
前記サーバと関連する動的負荷共有情報に基づいて、サーバネットワークの選択を決定する負荷共有ポリシーと、  
サーバネットワークの負荷を別のサーバネットワークに分散する方法を決定する分散ポリシーと  
のうちの 1 以上のポリシーを含む、請求項 3 9 記載の方法。

## 【請求項 4 1】

前記地政学に関するポリシーは、  
大陸ベースのポリシーと、  
国ベースのポリシーと、  
領域ベースのポリシーと、  
時間帯ベースのポリシーと  
のうちの少なくとも 1 つを含む、請求項 4 0 記載の方法。

## 【請求項 4 2】

調整ポリシーをさらに備える、請求項 4 1 記載の方法。

## 【請求項 4 3】

前記回答を決定するステップは、  
前記クライアントの地理上の所在位置を決定するステップと、  
前記クライアントの地理上の所在位置に関連する 1 以上のポリシーを検索するステップと、  
前記検索された 1 以上のポリシーに基づいて前記サーバネットワークを特定するステップと、  
前記選択されたサーバネットワークのドメインネームと CNAME とのうちの少なくとも 1 つを特定するステップと  
を備える、請求項 4 2 記載の方法。

## 【請求項 4 4】

前記少なくとも 1 つのポリシーを確立するステップをさらに備える、請求項 4 3 記載の方法。

## 【請求項 4 5】

前記少なくとも 1 つのポリシーを確立するステップは、  
適応型トラフィック制御 (ATC) 管理フレームワーク内の管理マスタエージェント (AMA) の適応型トラフィック制御 (ATC) ポリシー管理メカニズムにより、少なくとも 1 つのソースから前記少なくとも 1 つのポリシーを受信するステップと、  
前記サーバネットワーク内の 1 以上の管理対象サーバからの前記少なくとも 1 つのポリシーの動的ポーリングを行うステップと  
のうちの少なくとも 1 つを備える、請求項 4 4 記載の方法。

## 【請求項 4 6】

前記少なくとも 1 つのソースは、  
加入者と、  
調整エンティティと  
のうちの少なくとも 1 つを含む、請求項 4 5 記載の方法。

## 【請求項 4 7】

前記 ATC ネットワークサーバネットワーク内の前記少なくとも 1 つのドメインネームサーバへ前記少なくとも 1 つのポリシーを配信するステップをさらに備える、請求項 4 6 記載の方法。

## 【請求項 4 8】

更新されたポリシーを生成するべく、前記ポーリングステップによりポーリングされた

動的ポリシーに基づいてポリシーを動的に更新するステップと、

前記 A T C 名前サーバネットワーク内の前記少なくとも 1 つのドメイン名前サーバへ前記更新済みポリシーを配信するステップと

をさらに備える、請求項 4 7 記載の方法。

【請求項 4 9】

ドメイン名前サーバ内のモニタメカニズムにより、前記ドメイン名前サーバの作動状態をモニタするステップをさらに備える、請求項 4 8 記載の方法。

【請求項 5 0】

前記モニタするステップは、

前記ドメイン名前サーバの作動中に生じるイベントをモニタするステップと、

前記 A T C 管理フレームワーク内の A T C ネットワークモニタメカニズムへ前記イベントを送信するステップと

を備える、請求項 4 9 記載の方法。

【請求項 5 1】

前記モニタメカニズムによって、モニタ対象サーバまたは管理対象サーバのいずれかのサーバとして指定された 1 以上のサーバの利用可能性をモニタし、それによって、前記ドメイン名前サーバが、前記 1 以上のサーバの利用可能性に基づいて、前記サーバを決定することができるステップをさらに備える、請求項 5 0 記載の方法。

【請求項 5 2】

前記モニタメカニズムにより、前記サーバネットワーク内の 1 以上の管理対象サーバからの動的負荷共有情報または負荷分散情報のポーリングを行い、それによって前記ドメイン名前サーバが、前記動的負荷共有情報と前記負荷分散情報とに基づいて前記サーバを決定することができるステップをさらに備える、請求項 5 1 記載の方法。

【請求項 5 3】

前記 A T C 管理フレームワークにより、前記 A T C 名前サーバネットワークの作動状態を管理するステップをさらに備える、請求項 5 2 記載の方法。

【請求項 5 4】

前記管理するステップは、

前記 A T C 名前サーバネットワーク内のモニタメカニズムからイベントを受信するステップと、

前記 A T C ネットワークモニタメカニズムにより、前記ドメイン名前サーバから受信した前記イベントを統合して、統合されたイベントを生成するステップと、

前記統合されたイベントを処理するステップと

を備える、請求項 5 3 記載の方法。

【請求項 5 5】

前記処理するステップの結果に基づいて警告を生成するステップと、

前記 A T C 管理ネットワークのネットワークオペレーションセンタと加入者とへ警告を送信するステップと

をさらに備える、請求項 5 4 記載の方法。

【請求項 5 6】

コンテンツプロバイダのリソースが、加入者サーバネットワークと前記加入者サーバネットワークとは異なる少なくとも 1 つのコンテンツ配信ネットワーク ( C D N ) とを含む少なくとも 2 つの異なるサーバネットワークからクライアントへ配信されるフレームワーク内で操作可能な、ホスト名を解決する方法であって、

適応型トラフィック制御 ( A T C ) 名前サーバネットワーク内のドメイン名前サーバによって、リゾルバを介してクライアントからのホスト名の解決を求める要求を受信するステップと、

前記クライアントの地理上の所在位置と、少なくとも 1 つのポリシーとに少なくとも部分的に基づいて、( a ) 前記少なくとも 1 つのコンテンツ配信ネットワークと ( b ) 前記加入者サーバネットワークとのいずれか 1 つを選択するステップと、

少なくとも1つの所在位置ベースのポリシーに基づいて、前記選択されたサーバネットワークのドメイン名とCNAMEとのうちの少なくとも1つを決定するステップと  
を備える、方法。

【請求項57】

前記加入者サーバネットワークは、少なくとも1つのサーバグループを含む、請求項56記載の方法。

【請求項58】

個々のサーバグループは、  
少なくとも1つの一次サーバを備える第1層と、  
前記少なくとも1つの一次サーバが機能しなくなった場合に機能する1以上の第1のレベルのオーバーフローサーバを備える第2層と、  
前記少なくとも1つの一次サーバと、前記1以上の第1のレベルのオーバーフローサーバとの双方が機能しなくなった場合、1以上の第2のレベルのオーバーフローサーバを備える第3層と  
のうちの少なくとも1つを含むサーバ階層に対応する、請求項57記載の方法。

【請求項59】

前記サーバネットワーク内の個々のサーバは、  
モニタ対象サーバと、  
管理対象サーバと  
のうちの少なくとも1つを備え、  
前記モニタ対象サーバの利用可能性が動的にモニタされ、  
前記管理対象サーバの利用可能性が動的にモニタされるか、または前記管理対象サーバの負荷共有もしくは負荷分散が動的にモニタされる、請求項58記載の方法。

【請求項60】

前記少なくとも1つのポリシーは、  
前記クライアントの地理上の位置に基づいて、サーバネットワークの選択を決定する地政学に関するポリシーと、  
前記サーバネットワークと関連する動的負荷共有情報に基づいて、サーバネットワークの選択を決定する負荷共有ポリシーと、  
サーバネットワークのサーバの負荷を別のサーバネットワークに分散する方法を決定する分散ポリシーと、  
調整ポリシーと  
のうちの1以上を含む、請求項59記載の方法。

【請求項61】

前記サーバネットワークを選択するステップは、  
前記クライアントの地理上の所在位置を決定するステップと、  
前記クライアントの地理上の所在位置に関連する1以上のポリシーを検索するステップと、  
前記検索された1以上のポリシーに基づいて前記サーバネットワークを決定するステップと  
を備える、請求項56記載の方法。

【請求項62】

前記少なくとも1つのポリシーを動的に確立するステップをさらに備える、請求項61記載の方法。

【請求項63】

前記少なくとも1つのポリシーを確立する前記ステップは、  
適応型トラフィック制御(ATC)管理フレームワーク内の管理マスタエージェント(AMA)の適応型トラフィック制御(ATC)ポリシー管理メカニズムから配信される前記少なくとも1つのポリシーを受信するステップと、  
前記サーバネットワーク内の1以上の管理対象サーバから1以上の負荷共有ポリシーま

たは負荷分散ポリシーの動的ポーリングを行うステップと、

更新されたポリシーを生成するべく、前記 A T C ポリシー管理メカニズムから受信されるか、または管理対象サーバからポーリングされる、対応する動的ポリシーに基づいてポリシーを更新するステップと

のうちの少なくとも1つを備える、請求項 6 2 記載の方法。

【請求項 6 4】

前記ドメインネームサーバのモニタメカニズムにより、前記ドメインネームサーバの作動状態をモニタするステップをさらに備える、請求項 6 3 記載の方法。

【請求項 6 5】

前記モニタステップは、

前記ドメインネームサーバの作動中に生じるイベントをモニタするステップと、前記 A T C 管理フレームワーク内の A T C ネットワークモニタメカニズムへ前記イベントを送信するステップと

を備える、請求項 6 4 記載の方法。

【請求項 6 6】

モニタ対象サーバまたは管理対象サーバのいずれかのサーバとして指定された1以上のサーバの利用可能性をモニタし、それによって前記ドメインネームサーバが、前記1以上のサーバの利用可能性に基づいて前記サーバを決定できるステップをさらに備える、請求項 6 5 記載の方法。

【請求項 6 7】

前記少なくとも1つのポリシーに対する考慮は、前記コンテンツプロバイダによって設定される、請求項 1 から 4 のいずれかに記載のフレームワーク。

【請求項 6 8】

前記選択されたネットワークと関連する情報は、前記選択されたネットワークと関連するドメインネーム、または前記選択されたネットワークと関連する C N A M E を含む、請求項 1 から 4 および 6 7 のいずれかに記載のフレームワーク。

【請求項 6 9】

前記少なくとも1つのポリシーに対する考慮は、前記ネットワークの各々に対する相対的負荷共有を特定する負荷共有ポリシーを含み、前記選択するステップは、前記負荷共有ポリシーを満たすように試みる、請求項 1 から 4、6 7 および 6 8 のいずれかに記載のフレームワーク。

【請求項 7 0】

前記少なくとも1つのポリシーに対する考慮は、前記コンテンツプロバイダによって更新される、請求項 1 から 4、6 7 から 6 9 のいずれかに記載のフレームワーク。

【誤訳訂正 2】

【訂正対象書類名】明細書

【訂正対象項目名】全文

【訂正方法】変更

【訂正の内容】

【発明の詳細な説明】

【発明の名称】構成可能な適応型広域トラフィック制御および管理

【技術分野】

【0001】

本特許文献には著作権の保護を受ける情報が含まれる。本著作権所有者は、アメリカ合衆国において複製が行われるとき、何人が行う本特許文献または本特許のファクシミリによる複製に対しても異議を申し立てない。しかしながら特許商標庁のファイルまたは記録については別様に著作権上の権利を保留するものとする。

【0002】

本発明の態様はネットワークトラフィックの管理に関する。本発明の別の態様は、インターネットなどのネットワークにおける構成可能な適応型広域トラフィックの制御と管理

とに関する。

【背景技術】

【0003】

インターネットによるトラフィック量が大きくなるにつれて、ウェブコンテンツとアプリケーションのプロバイダは、高いトラフィック負荷の下で良好なエンドユーザ経験を維持するために、広範囲にわたる別個の位置に置かれた複数のサーバからのコンテンツの配信がますます必要となる。このことによって、いくつかの困難な挑戦すべき課題が生じることになるが、中でも、以下の課題が挙げられる。即ち、1以上の個々のサーバの故障に直面した際にこのような複数サーバシステムのフォールトトレランスを保證する方法と、経済上、契約上あるいは別の理由のために課せられる重要なコンテンツプロバイダポリシーの制約条件に基づいて個々のサーバへエンドユーザからの要求を分散する方法を制御する方法と、ネットワーク状態が変化したときエンドユーザが経験するような高いパフォーマンスを保證する方法と、である。

【発明の開示】

【課題を解決するための手段】

【0004】

本発明は、構成可能な規則のセットに基づいて、(インターネットなどの)ネットワークトラフィックを分散する手段を提供することによりこれらの問題並びにその他の問題を解決するものである。これらの規則は以下の重要なファクタを考慮に入れるように構成することが可能である。重要なファクタとは、サーバの利用可能性と、本発明を配備するコンテンツプロバイダの特定の要件(地勢、IPアドレス空間における位置、負荷共有などに基づく分散など)と、ネットワーク待ち時間の測定を含む、任意の所定時点におけるネットワーク(インターネット)の状態と、である。

【0005】

これらの規則は、一体として、インターネットコンテンツとアプリケーションのプロバイダへ非常にきめ細かなレベルのネットワークインターネットトラフィック制御を提供するものであり、これによってプロバイダは、従来方式のウェブサーバおよびミラー化されたサーバファームとにより提供されるエンドユーザ経験を上まわるエンドユーザ経験(要求解決のスピードと、関連するダウンロード時間と、サーバの利用可能性とにより測定される)の劇的改善を図ることが可能となる。

【0006】

本発明に対する多くの潜在的用途が存在する。1つの用途として、単一の組織が管理する1セットの指定サーバ向けに専らトラフィックを送るスタンドアローン型サービスの提供がある。本発明は、例えば、1以上の指定された宛先が、組織の制御の外側にあるサーバ(またはサーバのコレクション)を参照することができるようにさらに一般的な利用も可能である。後者の場合、例えば、潜在的宛先としてコンテンツ配信ネットワーク(CDN)並びにローカルな負荷・バランス用サーバが含まれる。コンテンツ配信ネットワーク自体のDNS(ドメインネームサービス)のコンポーネントを提供するために本発明を利用することが可能である。本発明は加入者向けサービスとして配備することが可能である。あるいは、加入者自身が直接利用するソフトウェアとして展開することが可能である。

【0007】

図面と関連して詳細に記載する実施形態例に関して本発明をさらに説明する。これらの実施形態は、本発明を限定しない実施形態例であり、全ての図面において、同様の参照番号は同様の部分を表すものとする。

【発明を実施するための最良の形態】

【0008】

詳細な実施例と関連して以下本発明について説明する。多種多様の形態で本発明を具現化できることが明らかになるが、これらの形態のいくつかは、開示された実施形態の形態とはきわめて異なるものとなる場合もある。したがって、本願明細書に開示された具体的な構造および機能の細部は単に典型的なものであり、本発明の範囲を限定するものではな

い。

【0009】

本発明を配備できる複数の様々なシナリオが存在するが、本説明は、記載を明瞭にするために、また、専ら例示を旨として、コンテンツプロバイダまたはアプリケーションプロバイダのために、サードパーティがDNSサービスを提供するシナリオに焦点を合わせるものである。

【0010】

図1は、本発明の種々の実施形態による高レベルのフレームワークまたはシステム100を示すものである。加入者102は、1以上のサーバグループ106-1~106-k(まとめて106)から構成される加入者サーバネットワーク104を介してコンテンツを提供する。

【0011】

本説明で用いられているように、本発明の種々の実施形態によるフレームワークでは、以下の3つのグループのユーザが想定されている。即ち、インターネットを利用してコンテンツおよび/またはアプリケーションにアクセスすることを望むエンドユーザと、管理対象コンピュータネットワーク上でサービスを提供し、サポートする通信事業者と、エンドユーザの要望をサポートするのを助けるために通信事業者のサービスに加入する加入者(通常コンテンツおよび/またはアプリケーションプロバイダ)とである。

【0012】

エンドユーザ、通信事業者、加入者という用語は、上記3つの役割を区別するためにこの本説明を通じて使用される。ただし、単一のエンティティにより2以上の役割が行われる多くのシナリオが存在する。このようなシナリオが本発明により想定されている。

【0013】

個々のサーバグループ106は、サーバの1以上の層を含むサーバ階層に対応することができる。例えば、サーバ階層の第1層は、1以上の一次サーバを含むことができ、サーバ階層の第2層は、第1層の一次サーバが正しく機能できない場合に使われる1以上のオーバーフローサーバを備えることができる。一般に、j番目のサーバグループの場合、サーバグループ106-jの第1層の一次サーバは108-jと表示され、サーバグループ106-jの第2層のオーバーフローサーバは110-jと表示される。

【0014】

サーバグループ内の個々のサーバは、クライアントからなどの要求に回答してリソースを提供する任意の処理プロセスまたは処理プロセスのコレクションである。サーバはいずれの既製のウェブサーバであってもよい。実施形態によっては、サーバがアパッチサーバやネットスケープコミュニケーション社のサーバなどのようなウェブサーバであるものもある。

【0015】

クライアント112は、加入者からコンテンツを取得するために、加入者サーバネットワーク104にアクセスする。コンテンツには、ビデオデータおよび音声データ等を含む任意の種類が制限なしで含まれる。このアクセスを行うために、クライアント112のユーザはユニバーサルリソースロケータ("URL")などのリソースロケータをクライアント112のブラウザ114に入力する。URLはネットワーク上のリソース(情報、データファイルなど)の所在位置を指定する。URLは、T. Berners-Leeらのユニフォームリソースロケータ(URL)(ネットワーク作業グループ、コメント要求:1738、カテゴリ:トラック規格、1994年12月:"http://ds.internic.net/rfc/rfc1738.txt",)に詳細に定義されている。これは本願明細書で参照により援用されている。URLは、以下のフォームを有する:スキーム:/host[:port]/url-path。この場合、スキームは"ファイル"(ローカルなシステム上のファイルを表す)や、"ftp"匿名FTPファイルサーバ上のファイルを表す)や、"http"(ウェブサーバ上のファイルを表す)や、"telnet"(Telnetベースのサービスとの接続を表す)などのシンボルとする

ことができる。その他のスキームも利用可能であり、新たなスキームが時々追加される。ポート番号はオプションであり、ポート番号が設けられていなければ、(スキームに応じて)システムがデフォルトのポート番号に取り替える。"host"フィールド(ホスト名)は、特定のコンピュータ用の1以上の特定のネットワークアドレスへの対応づけを行う。"url-path"は"host"フィールドで指定されたコンピュータに対する相対的なフィールドである。url-パスは(但し必ずしもこれに限定されるものではないが)通常ウェブサーバディレクトリ内のファイルのパス名である。

【0016】

フレームワークまたはシステム100には少なくとも1つのドメインネームサービス(DNS)のネームサーバ118-1が含まれる。好ましい実施形態では、システム100は、特定の単一エンティティがすべて作動するDNSネームサーバ118-1、118-2~118-n(まとめてネームサーバ118と呼ぶ)も備える。図1に図示の実施形態では、ネームサーバのうちの1つ118-1は米国用として機能し、別のネームサーバ118-2は英国用として機能し、別のネームサーバ118-3は日本用として機能する、等々。様々なネームサーバ118-1、118-2~118-nを(まとめてまたは個々に)構成して、地理領域、地政学領域、企業構造またはその他の任意の論理的編成構造として機能させることが可能である。個々のネームサーバ118の構造と動作について以下説明する。

【0017】

クライアントのブラウザ114が(URLの形などで)要求を取得すると、ブラウザは、要求されたURLで指定されたホスト名のアドレスを求めてブラウザのリゾルバ116に対する問合せを行う。リゾルバ116は最終的に特定のネームサーバ(ネームサーバ118-1など)に対する問合せを行う。ネームサーバ118-1は、加入者サーバネットワークのサーバ(または複数のサーバ)のIP(インターネットプロトコル)アドレス(または複数のアドレス)を返信する(出力するまたは出力を試みる)。リゾルバ116へ返信される特定のIPアドレスの決定は、(リゾルバのIPアドレスから決定されるような)リゾルバの所在位置および様々なポリシー(加入者ポリシー120、その他のポリシー122など)の複数のファクタに基づいて行うことも可能である。次いで、クライアントのブラウザ114は、所望のリソースを取得するために、加入者サーバネットワーク内の選択されたサーバと交信することができる。

【0018】

本発明の種々の実施形態によるネームサーバ118-1、118-2~118-nは、適応型トラフィック制御(ATC)メカニズム126を備え、このATCメカニズム126はポリシーデータベース124内のポリシーに基づいてドメインネームサービスをクライアントに提供する。個々のネームサーバ118は、クライアントの要求をクライアントの所在位置と関連づける所在位置決定メカニズム128へのアクセスを含み、あるいは、このアクセスを行う。このようなメカニズム128は、ケーブル&無線PLC社のTraceWare(登録商標)製品などであってもよい。TraceWare(登録商標)は、インターネット消費者の発信国、領域および大都市エリアを認識するその能力によってリアルタイムの、地理的人工知能(intelligence)を与えるインターネット地図帳を提供するサービスセットである。

【0019】

加入者サーバネットワーク104は、内在的な加入者のために、インターネットコンテンツまたはサービスを提供するサーバネットワークを表す。例えば、加入者は、インターネットを介してエンドユーザのブラウザへコンテンツを配信する自身のサーバネットワークを有するコンテンツプロバイダになることができる。ある判断基準に基づいて、サーバネットワーク104内のすべてのサーバ間でサービス要求の処理を合理的に分散できるように加入者サーバネットワーク104を構成することができる。上記分散を行うために、例えば、1以上のサーバグループ(サーバグループ1 106-1~サーバグループk 106-kなど)を備えるように加入者サーバネットワーク104の編成を行うことがで

きる。上記個々のサーバグループがサービス要求の一部を処理する責任を負うようにすることも可能である。例えば、フィンランドから着信するサービス要求は、ヨーロッパに物理的に配置されたサーバグループへ経路指定を行うことも可能である。

#### 【0020】

加入者サーバネットワーク104内の個々のサーバグループ106はさらに負荷を共有する複数のサーバを設けるようにすることも可能である。例えば、フィンランドからのサービス要求は、スカンジナビアに配置されたサーバへ次に経路指定を行うことも可能である。異なるサーバグループへの、および、その後の異なるサーバへのルート指定サービス要求を様々な判断基準に基づいて行うようにすることも可能である。例えば、要求元とサーバの所在位置との間の距離に基づいて上記のようなルート指定を行うことも可能である。例えば、フィンランドから発信されたサービス要求の場合、米国に配置されているサーバへ向けて送る代わりに、ノルウェーに配置されているサーバへ向けてこの要求を送る方が効率がよくなることが考えられる。サーバ負荷を用いて、サービス要求の経路指定を行う場所を決定することも可能である。例えば、米国内のサーバグループが過負荷状態にあり、一方メキシコにあるサーバが比較的アイドルな状態であれば、米国から発信されたサービス要求をメキシコにあるサーバグループへ経路指定することも可能である。

#### 【0021】

サーバグループ内のサーバを編成して、サーバからなる1以上の層を備えた階層にすることも可能である。異なる層におけるサーバが、異なる指定目的を持つようにすることができる。例えば、サーバ階層の第1層のサーバは一次機能サーバであるサーバを設けることができ、第2層のサーバは、第1層の一次サーバが利用できなくなったり、過負荷状態になったりした場合にのみアクティブになるオーバーフローサーバとして使用するサーバを設けることができ、さらに、第2層オーバーフロー用として使用する第3層のサーバは、第2層の一次サーバとオーバーフロー（または第1層オーバーフロー）サーバとが利用できなくなったり、過負荷状態になったりした場合にのみアクティブになるサーバを設けることができる。

#### 【0022】

サーバグループ階層の第1層は1以上の一次サーバを備えることも可能である。複数の一次サーバが存在する場合、負荷を共有するようにこれらの一次サーバを構成することができる。例えば、5つの一次サーバが第1層に存在する場合、サーバグループへ経路指定した総サービス要求の20%を個々のサーバが受け取るようにこれらの一次サーバを構成することも可能である。このような一次サーバの個々のサーバの場合、特定のサーバが過負荷状態になったり、故障したりした場合、このサーバへ最初に指定した負荷共有を分散したり、別のサーバへ送信したりすることができるように上記個々のサーバをさらに構成することも可能である。サーバが過負荷状態でないとき、分散された負荷を構成することも可能である。他のサーバに対して分散する対象部分は或る予め定義したポリシーにより決定することができる。

#### 【0023】

上記のように、基底サーバの固有の機能に基づいてサーバグループ106内のサーバを異なるカテゴリに類別することも可能である。例えば、サーバグループ106内のサーバは、一次サーバ、第1層オーバーフローサーバ、または第2層オーバーフローサーバ、などであってもよい。サーバを動的にモニタするか否かという観点から、および、サーバを動的にモニタする方法という観点からサーバの類別を行うことも可能である。例えば、実施形態のなかには、モニタ対象サーバまたは管理対象サーバのいずれかとしてサーバを類別できるものもある。

#### 【0024】

モニタ対象サーバの類別は、その利用可能性に関連して基底サーバを動的にモニタすることを示す。この場合、ある予め定めたスケジュールに基づいてサーバをその利用可能性に関連してプローブすることも可能である。この利用可能性を正確に検出できるように、ネットワークの異なる位置から基底サーバへこのようなプローブを送信することができる

。すなわち、1つの位置から送られた基底サーバが1つのプローブに応答できなかった場合、必ずしも、サーバがそれ以上利用できないことを示すとはかぎらない（単にネットワークの一部の輻輳状態に起因する可能性もある）。

【0025】

プローブは異なる方法で実現することができる。プローブは、単に、確認応答の要求のためにサーバへ送信する信号にすぎない場合もある。プローブは、基底サーバ上の指定した位置に記憶されたファイルのポーリングを行うポーリング処理である場合もある。このファイルを首尾よくポーリングを行うことができた場合、基底サーバは利用可能であると考えられる。検出された利用可能性を用いて、ネットワークトラフィックの管理が、サーバと関連するダイナミクスに応答するようにサーバと関連するポリシーの調整や更新を行うようにすることが可能となる。

【0026】

管理対象サーバとして類別されたサーバは適応型ポリシーベースの管理方式にアクティブに参加することができる。モニタ対象サーバの場合と同様、その利用可能性に対して管理対象サーバを定期的にプローブすることができる。さらに、管理対象サーバはその負荷共有または分散された負荷に関連する情報を動的に提供することができる。管理対象サーバはその変更された容量またはその現在の負荷に基づいてその負荷共有または負荷分散部分を更新することができる。例えば、管理対象サーバがグレードアップされたとき、その負荷共有またはその負荷分散部分を増減できるようにその容量を増やすことができる。一方、管理対象サーバは、過負荷状態になった場合、その負荷共有を低いレベルへ改訂したり、故障を防止するためにその負荷分散部分を増やしたりすることができる。管理対象サーバは、サーバに記憶された指定ファイル内の対応する負荷共有または負荷分散情報を更新することにより、その負荷共有または分散された負荷を改訂することができ、さらに、このファイルをネームサーバによりポーリングして、動的に変更された負荷共有と負荷分散情報とを用いて、トラフィックを適宜送信できるようにすることも可能である。

【0027】

加入者サーバネットワーク104内での（クライアント112からの）サービス要求の分散は、ポリシーデータベース124に記憶された1セットのATCポリシー（120、122）を介して制御可能である。様々な当局者がATCポリシーに影響を与えることができ、ポリシーデータベース124内にポリシーを形成することが可能となる。例えば、加入者はポリシーを設定して、加入者のネットワーク104内の基底サーバの地理上の所在位置と容量などの考慮と関連してトラフィックを送信することができる。例えば、ネームサーバ118の通信事業者や様々な地政学上のエンティティを含む他のポリシーエンティティ138は、ネットワークトラフィックの管理および送信方法に関するポリシーを知ることができる。例えば、政府や何らかの組織のエージェントはネットワークトラフィックポリシーのいくつかの態様を調整することができる。このような調整ポリシーは、調整ポリシーを満たす方法でクライアント112からのサービス要求を経路指定できるように一体化を要求される場合がある。

【0028】

したがって、ポリシーデータベース124内のATCポリシーは、加入者ポリシー120と、加入者102とポリシーエンティティ138などの異なるソースから得られる別のポリシー122との組み合わせとすることができる。ポリシーデータベース124からATCメカニズム126によって異なるソースから得られるポリシーに、アクセスすることが可能である。ATCメカニズム126の方から見ると、ポリシーのソースは無関係のものであったり、決定できないものであったりする場合さえある。例えば、指定した位置に記憶したテキストファイルでポリシーを定義することも可能であり、ATC管理フレームワーク142内のATCポリシー管理メカニズム152へ上記のポリシーをダウンロードし、次いで、ATCネームサーバネットワーク140内の個々のネームサーバ内に配置されているデータベース管理者132へこのポリシーを配信することも可能である。このダウンロードは、グラフィックユーザインタフェース（GUI）、ファイル転送プロトコル

(FTP)または他の何らかのメカニズムのいずれかを介して行ってもよい。ポリシー作成者がウェブベースのGUIを介して直接ポリシーを入力してもよい。例えば、加入者102は、好ましくは("https"プロトコルなどを用いて実現された)機密保護を施したインタフェースを介してATC管理フレームワークと接続されるブラウザインタフェース156を介して加入者ポリシー120を入力することができる。

【0029】

ATCメカニズム126により使用されるポリシーデータベース124から得られるポリシーは、まとめてATCポリシーと呼ばれ、これらのポリシーは加入者ポリシー120並びにその他のポリシー122を含むことができる。但し、これらのポリシーに限定されるものではない。異なるレベルの加入者サーバネットワーク104においてトラフィックの決定および/または制御を行うようにATCポリシーを編成することも可能である。図2は本発明の種々の実施形態による例示タイプのATCポリシー200を示す。

【0030】

ATCポリシー(200)は、地政学ポリシー215、負荷共有ポリシー240、フェイルオーバーポリシー245、層化フェイルオーバーポリシー250、分散ポリシー255、調整ポリシー260、および、無階級ドメイン間ルート指定(CIDR)ブロックポリシー210などの異なるタイプのポリシーに類別することができる。

【0031】

ポリシーデータベース124内のこれらの例示ポリシーについて以下さらに詳述する。地理的ポリシー(215)：決定は、エンドユーザのリゾルバのIPアドレスなどを用いて、エンドユーザの所在位置またはその近似位置に基づいて行われる。例えば、IPアドレスが米国内であれば、要求は、加入者サーバネットワーク104内の"国内"グループのサーバへ向けて送信することができ、IPアドレスが米国内でなければ、上記ネットワーク内の"国際"サーバへ向けることができる。この要求は、独自のコンテンツ配信ネットワーク(CDN)または加入者が指定する別のサービスへ向けることも可能である。

【0032】

負荷共有ポリシー(240)：加入者は、加入者サーバネットワーク104内の定義されたサーバセット内の加入者のサーバの各々へ送信する対象トラフィック(負荷共有)量を明白に指定することができる。通常負荷は個々のサーバの容量に基づいて指定することができる。このような指定に基づいて、個々のサーバの負荷共有を総負荷の割合(%)として導き出すことができる。

【0033】

フェイルオーバーポリシー(245)：一次サーバのいくつか機能がなくなったフェイルオーバー状況に関して加入者はポリシーを指定することができる。このようなシナリオを処理するために、フェイルオーバーポリシーは、例えば、サーバの利用可能性をモニタする頻度、および、一次サーバの部分的セットが利用できないことが検出された場合に採るべき戦略に関してATCメカニズムに指示を与えることができる。例えば、フェイルオーバーポリシーは、別の一次サーバへ故障中のサーバの負荷を分散するように指定することができる。上記とは別に、フェイルオーバーポリシーは、一次サーバ以外のサーバへ向けてトラフィックを送信するようにATCフレームワークに指示することもできる。

【0034】

層化フェイルオーバーポリシー(250)：加入者は、前の層内の1以上の加入者サーバが機能しなかった場合、次の層のサーバへ向けて再送信すべき負荷を定める層化フェイルオーバーポリシーにより戦略を指定することができる。例えば、加入者サーバネットワークを定義する際に、一次サーバの第1層と、第1層オーバーフローサーバの第2層と、第2層オーバーフローサーバの第3層、などを含む階層として個々のサーバグループを構成することが可能である。この場合、層化フェイルオーバーポリシーを定義して、一次サーバからオーバーフローサーバへ向けて負荷を再送信すべき時点を指示することができる。例えば、層化フェイルオーバーポリシーは、すべての一次サーバが故障した場合、第2層へ負荷を送信すべきであること、さらに、第1層と第2層の双方のサーバが故障した場合、第3層の

オーバーフローサーバへ負荷を送信すべきであることを示すことができる。トラフィックも別の何らかのサーバへ再送信することができる。例えば、コンテンツ配信ネットワーク(CDN)が利用可能な場合、CDN全体へ向けてトラフィックを再送信することも可能である。

#### 【0035】

分散ポリシー(255)：状況によっては、あるサーバへ最初に指定した"負荷"の部分を1以上の異なるサーバに分散したり、そのようなサーバへ向けて再送信したりすることも可能である。加入者サーバに向けられたトラフィック量が予め規定したレベルを超えた場合に上記分散や再送信を行うことができる。これらのケースでは、上記規定したレベルを超えない場合にサーバへ向け送信されるトラフィック(分散された小部分)の加入者指定の小部分を1以上の他の異なるサーバに分散することも可能である。過負荷に起因して生じる破滅的な故障を防ぐために、このような戦略を採ることが可能である。分散対象負荷を受け取るサーバは、オーバーフローサーバまたはコンテンツ配信ネットワークのような別の何らかのサーバであってもよい。サーバの応答時間に基づいて過負荷状態を検出することができる。例えば、サーバからの応答時間が長くなれば、サーバが過負荷状態であることを示すことができる。この場合、どこか別の場所へトラフィックを再送信するために分散ポリシー255を呼び出すことができる。例えば、(0.3、0.3、0.4)の負荷共有を持つサーバグループ内に合計3つの一次サーバを設け、総負荷の40%を受け取るように指定されている一次サーバが完全に過負荷状態になった場合、分散ポリシーは、例えば、CDN105内に配置されているサーバへ向けて一次サーバの最初の負荷の50%を再送信することによりこのサーバの負荷を分散するように指定することができる。分散ポリシーは、分散用サーバへトラフィックの再送信を行う条件を指定することも可能である。このような条件は望ましいレベルの分散用サーバのパフォーマンスに関するものであってもよい。

#### 【0036】

CIDRポリシー(210)：IPアドレス空間のCIDRブロックに基づいてポリシー決定がサポートされている。CIDRは、無階級ドメイン間ルート指定を示し、クラスA、B、Cに基づいてシステムを置き換えるIPアドレス指定方式である。CIDRの場合、単一のIPアドレスを用いて多くの一意IPアドレスの指定を行うことが可能である。

#### 【0037】

調整ポリシー(260)：何らかのポリシーエンティティにより或るポリシーを指定して、ネットワークトラフィックを制御することも可能である。システム100においてこのようなポリシーを実施することも可能である。

#### 【0038】

ポリシーは静的ポリシーあるいは動的なポリシーいずれも可能である。加入者サーバネットワーク104からのサーバ選択は、適応型の、定期的に更新されるインターネットの状態マップに基づいて行うことも、適応的に更新されるポリシーに基づいて行うことも可能である。このマップは、IPアドレスのネットワーク待ち時間に基づいて選択されたセットのネットワークエージェントへIPアドレスをまとめてクラスタすることができる。これによって、エンドユーザのブラウザまでの加入者サーバの"ネットワークでの近接性(proxyimity)"に基づいて選択される加入者サーバの作動が可能となり、この結果ダウンロード時間の最適化が行われる。利用可能性と負荷などのサーバの動的状態を反映するこのような適応的方法で上記ポリシーを定義することができる。

#### 【0039】

地政学ポリシー215は、クライアントがどこに位置しているかに基づいてサーバの選択を決定することができる。図2に図示のように、地政学ポリシー215は、大陸ベース分散ポリシー220、国ベース分散ポリシー225、領域ベース分散ポリシー230および時間帯ベース分散ポリシー235にさらに類別することができる。これらのポリシーを設定して、異なる地理的または政治的判断基準に基づいて特定サーバグループを選択する

プロセスを決定することができる。

【0040】

地政学ポリシーは（上記記載の）負荷ベースポリシーとは異なる。前者は地理的判断基準または時間的判断基準に基づいて選択を案内するように設計されている。後者は基底サーバの動的容量と負荷とに関連する選択処理に関する。負荷共有ポリシー240はサーバの容量に基づいて選択を決定する。サーバグループ内の機能サーバが過負荷状態になったり、故障したりしたとき、部分的フェイルオーバーポリシーまたは層化フェイルオーバーポリシー（245と250）がトラフィック再送信処理プロセスを決定する。

【0041】

A T Cポリシー200を階層で構築して、決定ツリーを形成することができる。図3は、本発明の一実施形態による、例示の加入者ポリシー階層または種々のタイプのポリシーに基づいて構成される決定ツリーを示す図である。図3では、大陸ベースの分散ポリシー220を用いて、特定の大陸に限定された選択処理プロセスがまず送信される。例えば、要求元クライアント112がアジアに位置すれば、大陸ベースの分散ポリシー220は、アジアに配置されているサーバ内でさらなる選択処理を送信することができる。同様に、クライアント112が北米またはヨーロッパのいずれかに位置していれば、対応する大陸に配置されている適当なサーバへ向けてさらなる選択処理プロセスを送信することができる。

【0042】

一旦DNS要求が適切な大陸へ向けられると、国ベースの分散ポリシー225は、クライアント112が位置する同じ国または近くの国にある特定のサーバへさらに選択肢を制約することができる。例えば、クライアント112が米国内に位置する場合、国ベースのポリシー225は、アメリカ合衆国内に配置されているサーバから選択を送信することができる。同様に、領域ベースの分散ポリシー230は、クライアント112がどこに位置するかに応じて、例えば西海岸や東海岸などにさらに選択を制約することができる。

【0043】

特定サーバグループを選択した場合（大陸ベースのポリシー220に基づく階層決定と領域ベースのポリシー230の後など）、負荷共有ポリシー240は上記処理プロセスを決定することが望ましく、これにより、所定のサーバグループ内のサーバが選択される。このようなポリシーはサーバの容量に基づいて決定することもできる。あるいは基底サーバの動的パフォーマンスまたは負荷に基づいてこのようなポリシーを適宜改訂することができる。負荷共有ポリシー240は、サーバグループ内の個々のサーバが処理すべき総要求の（共有）割合（％）を指定することができる。例えば、サーバグループが合計の3つの一次サーバ（サーバ1、サーバ2、サーバ3）を含む場合、このサーバグループに対する負荷共有ポリシーは（0.3、0.5、0.2）として負荷共有を指定することが可能であり、これはサーバ1が総負荷の30％を受け取り、サーバ2が負荷の50％を受け取り、サーバ3が総負荷の20％を受け取るべきであることを示す。

【0044】

特定のデフォルトセットのサーバがそれ以上機能しないか、利用できなくなった場合に、層化フェイルオーバーポリシー250はサーバの選択を決定する。例えば、サーバグループ内の一次サーバは、作動が正常である場合、サービスを提供するデフォルトセットのサーバと考えることができる。サーバの応答時間に基づいてこのような一次サーバの利用不能性を検出することができる。例えば、サーバが単に応答していなければ、このサーバは利用できないと考えられるかもしれない。すべての一次サーバがダウンした場合、トラフィックをどこへ向けて送信すべきであるかが層化フェイルオーバーポリシー250により決定される。例えば、次の層のオーバーフローサーバへ向けてすべてのトラフィックを送信するように層化フェイルオーバーポリシー250を指定することができる。

【0045】

図4は、本発明の種々の実施形態による、加入者サーバネットワーク104と加入者ポリシー120との間の例示の関係を示す図である。ネットワーク階層またはツリーとして

加入者サーバネットワーク104が図4に示されている。このネットワークでは、加入者サーバネットワーク104は、サーバグループk106-kを通じてサーバグループ1106-1を含み、個々のサーバグループは、第1層内のそれ自身の一次サーバグループ1108と、第2層内のオーバーフローサーバグループ1110とを含む(例えば、サーバグループ1106-1は、一次サーバグループ1108-1と、これと関連するオーバーフローサーバグループ1110-1とを含む)ことができ、一方、サーバグループk106-kは、一次サーバグループ1108-kと、この一次サーバグループ1108-kと関連するオーバーフローサーバグループ1110-kとを含む。

【0046】

加入者ポリシー120は、クライアント112(リゾルバ116)からのDNS要求に回答してサーバのIPアドレスを返信できるように、加入者サーバネットワーク104内の(または別のあるサーバネットワーク内の)1以上のサーバの選択を決定する。加入者サーバネットワーク104において適切なサーバを決定したり、適切なサーバを選択したりするために、決定は階層で行うことができる。例えば、図4に図示のように、加入者サーバネットワーク104のレベルで、ATCメカニズム126は地政学上の分散決定410を行って、どのサーバグループを選択すべきかを決定することができる。一旦特定のサーバグループが選択されると、ATCメカニズム126は、例えば、サーバグループ内のサーバ間でトラフィック負荷を共有すべき方法に基づいてグループ内のどの特定のサーバを選択すべきかをさらに決定することができる。サーバグループレベルでの決定は負荷共有ポリシー240に基づくものであってもよい。この意思決定処理は、サーバ階層内の個々のブランチノードにおいて、適切なATCポリシーを適用して、適切な単数のサーバまたは複数のサーバの選択を決定できることを示す。

【0047】

図4に例示のように、地政学ポリシー215を適用して、特定サーバグループと、負荷共有ポリシー240と、層化フェイルオーバーポリシー245と250との選択を制御することができる。分散ポリシー255を適用して、トラフィックを再送信することができる。すなわち、加入者サーバネットワーク104はツリーを形成し、ATCポリシー200はツリーの最上部からツリーの1以上のリーフまでのフローを決定する。ATCメカニズム126はATCポリシー200を適用することによりフローの制御を行う。

【0048】

図5は本発明の種々の実施形態による適応型トラフィック制御(ATC)フレームワークの高レベルのアーキテクチャを示す図である。ATCフレームワークはATC管理フレームワーク142とATCネームサーバネットワーク140を有する。ATC管理フレームワーク142は、加入者または別のポリシー作成エンティティ(138)と関連する様々な管理上のタスクに責任を負うものであり、上記タスクには、ATCポリシー200の操作と記憶、ATCネームサーバネットワーク140におけるネームサーバへのATCポリシー200の伝播または配信、ネームサーバの行動のモニタ、適切な媒体にモニタ結果を表示するための状態レポートの作成、ネットワークオペレーションセンタ(NOC)148(図1を参照)と加入者102への警告の送信が含まれる。

【0049】

ATCネームサーバネットワーク140は、DNS要求への応答に対して責任を負うものであり、このATCネームサーバネットワーク140には、DNS要求の処理と、加入者サーバネットワーク(または異なる指定されたネットワーク)から1以上のサーバを選択するためにATCポリシー200を適用する処理と、選択したサーバのIPアドレスによる応答処理とが含まれる。ATCネームサーバネットワーク140によって、ATC管理フレームワーク142からの受信か、サーバの動的作動状態による更新かのいずれかを受けるATCポリシー200を動的に維持される。ATCネームサーバネットワーク140により、動的に更新されたATCポリシー200に基づいてドメインネーム/IPアドレスの解決される。ATCネームサーバネットワーク140は、ネットワーク内の個々のネームサーバの作動状態をモニタし、ログデータとモニタデータとをATC管理フレーム

ワーク 142 へ供給することも可能となる。

【0050】

A T C 管理フレームワーク 142 はフォールトトレランスを持つように設計することができる。例えば、図 1 と図 5 とに示されているように、A T C 管理フレームワーク 142 は、管理マスタエージェント (A M A) 144 と、1 以上の A M A バックアップ 146 - 1 ~ 146 - m (まとめて 146) とを備えることができる。マスタエージェント 144 とバックアップ 146 とを備えたすべての A M A エージェントは正確な機能を実行することができるものであるが、これらの機能 (マスタ A M A 144 など) のうちの 1 つを中心的すなわち一次の管理マスタエージェントとし、その他の機能 (A M A バックアップ 146 など) をバックアップ用すなわち 2 次的または冗長なマスタエージェントとすることができるという点を除くものとする。中心的すなわち一次的 A M A 144 は A M A バックアップエージェント 146 を定期的にバックアップする責任を負うことができる。何らかの理由のために、一次 A M A 144 がそれ以上正しく機能しなくなった場合、A M A バックアップ 146 のうちの 1 つが中心的役割すなわちマスタ A M A 144 の役割を引き受けることができる。

【0051】

A T C ネームサーバネットワーク 140 は複数のネームサーバエージェント 118 - 1、118 - 2 ~ 118 - k を含むことが可能であり、これらのエージェントの各々は、特定の地理的 (または他の任意の管理上または機能上の) 領域の D N S 要求に対する責任を負うように設計することも可能である。例えば、ネームサーバエージェント 118 - 1 は、北米からのすべての D N S 要求を処理する責任を負うことが可能であり、ネームサーバ 118 - 2 はヨーロッパの D N S 要求に対して責任を負うことが可能であり、ネームサーバ 118 - 3 は日本からの D N S 要求に対して責任を負うことが可能である。さらに、ネームサーバエージェントは、ネットワーク内の別のネームサーバエージェントのためのバックアップ用ネームサーバエージェントとして使用することも可能である。例えば、北米のネームサーバエージェントが正しく機能しなくなった場合、ヨーロッパのネームサーバエージェントを北米からの D N S 要求の処理に一時的に割り当てることができる。その目的のために、A T C ネームサーバネットワーク 140 内のネームサーバエージェントのすべてへ A T C ポリシーをすべて伝えることができる。

【0052】

図 6 は、本発明の種々の実施形態による管理マスタエージェント (A M A) 144 の高レベル機能ブロック図を示すものである。A M A 144 は、機密保護を施したウェブベースのグラフィックユーザインタフェース 160 と、ポリシー編集メカニズム 162 と、A T C ポリシーデータベース 124 と、管理ポリシー更新メカニズム 164 と、A T C 管理ブラウザ 166 と、A T C ポリシー管理メカニズム 152 と、レポート作成メカニズム 168 と、A T C ネットワークモニタメカニズム 150 と、管理マスタバックアップメカニズム 170 とを有する。

【0053】

A T C ポリシーデータベース 124 は A T C ポリシー 200 を記憶する。上記のように、A T C ポリシー 200 は、異なるソースからの (加入者からのポリシーおよびネットワークトラフィックを制御する別のエンティティからのポリシーなどの) ポリシーを含むことも可能である。加入者ポリシー 120 と別のポリシー 122 の双方を定義し、A M A 144 へ提供することも可能である。図 6 に図示の例示の構成では、機密保護を施したウェブベースの G U I 160 を通じて A M A 144 でポリシーを受信することができる。A M A 144 へポリシーを配信することができる別の手段を設けることも可能であり、これについては後程論じる。ポリシー編集メカニズム 162 は、受信したポリシーを編成して、A T C ポリシー 200 を形成し、次いで、A T C ポリシーデータをベース 124 内に上記 A T C ポリシーを記憶する。

【0054】

A T C ポリシー管理メカニズム 152 は、A T C ネームサーバネットワーク 140 内の

関連するネームサーバへ A T C ポリシー 2 0 0 を配信または伝播し、それによって、A T C ポリシー 2 0 0 を用いて、ドメインネーム 翻訳サービスを制御できるようにしてもよい。異なる手段を介して記憶済み A T C ポリシーの動的更新を行うことができる。例えば、A T C 管理ブラウザ 1 6 6 を介してポリシーを更新することも可能である。あるいは管理ポリシー更新メカニズム 1 6 4 は既存の A T C ポリシーの改訂を行うことも可能である。

【 0 0 5 5 】

上記とは別に、A T C ポリシー管理メカニズム 1 5 2 を介して異なるソースから得られるポリシーを A M A 1 4 4 に設けることも可能であり、上記管理メカニズムは異なる位置からの動的に更新されたポリシーの定期的ポーリングを行うことができる。このような位置は、動的ポリシー関連情報を出力するように指定されたネットワーク位置、または、管理対象サーバとして類別されるサーバ（加入者サーバネットワーク 1 0 4 内か、C D N 1 0 5 内かのいずれかに在る）を含むことも可能である。例えば、サーバは、サーバに記憶された指定ファイルを介してその負荷共有を動的に指定することも可能である。このような動的に定義された負荷共有情報を管理対象サーバから検索するために、A T C ポリシー管理メカニズム 1 5 2 は、管理対象サーバに記憶された指定ファイルのポーリングを行って、関連する負荷共有情報を取得することができる。別のポリシー作成エンティティから動的ポリシーのポーリングを行うことも可能である。

【 0 0 5 6 】

A T C ポリシーの配信は、ある予め定義した間隔に基づいて周期的に行うことが可能であり、あるいは、記憶された A T C ポリシーが更新されるときはいつでも A T C ポリシーの配信をトリガーすることが可能である。A T C ポリシー管理メカニズム 1 5 2 は、既存の A T C ポリシーに対して行われる変化をモニタすることができる。A T C ポリシー管理メカニズム 1 5 2 は、A T C ポリシーデータベースに記憶された A T C ポリシーのポーリングを行い、変化が生じているかどうかを調べることができる。一方、指定した位置（このような位置は既存 A T C ポリシー内で指定することができる）から A T C ポリシー管理メカニズム 1 5 2 が動的ポリシーのポーリングを行うときはいつでも、上記管理メカニズムは、動的にポーリングされたポリシーが既存の A T C ポリシーと異なっているかどうかを決定することができる。更新されたポリシーが既存 A T C ポリシーと異なっている場合、A T C ポリシー管理メカニズム 1 5 2 は、A T C ネームサーバネットワーク 1 4 0 へ更新済みの A T C ポリシーを再配信することができる。

【 0 0 5 7 】

A T C ネットワークモニタメカニズム 1 5 0 は、A T C ネームサーバネットワーク 1 4 0 内の異なるネームサーバから D N S ログの要約を収集することができる。このような要約ログデータは、例えば、所定の時間内に特定のサーバへ向け送信された要求の数などの情報を提供するイベントの形で受信することができる。A T C ネットワークモニタメカニズム 1 5 0 は、A T C システム全体からのこのような D N S ログの要約（またはイベント）をまとめて処理することができる。レポート作成メカニズム 1 6 8 はこれらの要約からモニタ状態レポートを作成することが可能であり、機密保護を施したウェブベースの G U I 1 6 0 を介してこのようなレポートを加入者 1 0 2 が利用できるようにする。

【 0 0 5 8 】

管理マスタバックアップメカニズム 1 7 0 は、A M A バックアップ 1 4 6 - 1 ~ 1 4 6 - m を周期的に更新して、すべてのバックアップエージェントが最新のものであることを保証することができる。この周期的に更新には、A T C ポリシーと、様々な制御メカニズム（A T C ポリシー管理メカニズム 1 5 2 を含む）の作動状態、ポリシー編集メカニズム 1 6 2、管理ポリシー更新メカニズム 1 6 4 とのそれぞれの複製化、および、最新情報の提供を含むことができる。

【 0 0 5 9 】

管理マスタエージェントの主機能として、A T C ポリシーの管理と、A T C ネームサーバネットワーク 1 4 0 内のネームサーバエージェントへの更新済み A T C ポリシーの供給の確認と、システムパフォーマンスの動的モニタ状態レポートを作成する様々なネームサ

サーバのパフォーマンスのモニタと、ポリシーの動的更新が可能で、モニタレポートのチェックができる接続の維持とが挙げられる。

【0060】

システムエラーおよびその他の異常条件を示すフラグ情報は、ATCネットワークモニタメカニズムまたはエージェント150により収集される。図7は、本発明の種々の実施形態によるATCネットワークモニタメカニズム150の内部機能ブロック図を示すものである。ATCネットワークモニタメカニズム150は、トラップハンドラ176と、処理メカニズム182と、警告生成メカニズム184とを含む。トラップハンドラ176は、ネームサーバネットワーク140内のネームサーバからイベントをトラップする。処理メカニズム182はトラップされた収集済みイベントを分析し、次いで、この分析情報に基づいて、必要な場合、警告生成メカニズム184による警告が生成される。次いで、ATCのネットワークオペレーションセンタ(NOC)148と加入者102(図1)などへこのような警告を報告する。

【0061】

トラップハンドラ176は、ネームサーバからイベントをトラップするイベント受信装置178と、トラップされたイベントを類別し、合理的かつ適切な方法でこれらのイベントを編成できるイベント統合メカニズム180とをさらに備える。処理メカニズム182は統合化されたイベントを処理して、有用なパターンあるいは情報を与えるパターンを特定することができ、これらのパターンはさらに警告生成メカニズム184により用いられて、システムのパフォーマンスに著しい影響を与える可能性のある厄介な問題を含むパターンの特定を行うことができる。

【0062】

本発明に基づく適応型トラフィック制御(ATC)フレームワークは、別のコンテンツ配信ネットワーク(CDN)プロバイダと共に、または、別の任意のサービスと共に、ただ加入者のサーバのみへトラフィックを向けて送信するスタンドアロン型サービスとして展開することも可能である。

【0063】

ATCネームサーバネットワーク140内の個々のドメインネームサーバには、所在位置決定装置128、適応型トラフィック制御(ATC)メカニズム126、モニタエージェントまたはメカニズム130、データベース管理者132およびレポート作成装置134を設ける(図1)ことができる。ネームサーバ(118-1など)がクライアント112のリゾルバ116から要求を受信すると、所在位置決定装置128がリゾルバの位置を決定し、ATCメカニズム126へこのような所在位置情報を送信する。この所在位置情報に基づいて、ATCメカニズム126は、ポリシーデータベース124(加入者ポリシー120または別のポリシー122など)から関連するATCポリシーを検索し、検索された関連するポリシーに基づいて加入者サーバネットワーク104内の1以上のサーバを選択する。次いで、対応するIPアドレスまたは選択済みサーバのCNAMEがリゾルバ116へ返信される。

【0064】

データベース管理者132はポリシーデータベース124の保守管理を行う。データベース管理者132は、ATC管理フレームワーク142内のATCポリシー管理メカニズム152からポリシーを受信し、このポリシーをポリシーデータベース124にポピュレートする。ATC管理フレームワーク142から受信したATCポリシーは、加入者サーバネットワーク104(またはCDN105)においてサーバを定義または類別する情報を含むことができる。例えば、モニタ対象サーバと定義できるサーバもあれば、管理対象サーバに対応するサーバもある。

【0065】

データベース管理者は、このような情報を受信すると、基底サーバの類別に関する情報をモニタメカニズム130に与えることができ、その結果、個々のサーバの状態に基づいてモニタメカニズム130は個々のサーバのモニタを行うことが可能となる。ATCポリ

シー管理メカニズム 1 5 2 が更新されたポリシーを配信すると、データベース管理者 1 3 2 はポリシーデータベース 1 2 4 に記憶された関連するポリシーを適宜更新する。

【 0 0 6 6 】

モニタメカニズム 1 3 0 は加入者サーバネットワーク内のネームサーバ 1 1 8 - 1 と 1 以上のサーバの作動状態をモニタする。モニタメカニズム 1 3 0 は、作動中ネームサーバ 1 1 8 - 1 内で生じたイベントを収集し、A T C 管理フレームワーク 1 4 2 内の A T C ネットワークモニタメカニズム 1 5 0 へこのようなイベントを送信することができる。一方で、モニタメカニズム 1 3 0 は、個々のサーバが定義されている態様（モニタ対象サーバが管理対象サーバのいずれか）に応じて、加入者サーバグループ 1 0 4 内の（または C D N 1 0 5 内の）様々なサーバの処理をモニタすることができる。

【 0 0 6 7 】

サーバがモニタ対象サーバとして定義されている場合、モニタメカニズム 1 3 0 は（前述したように）サーバを動的にプローブしてその利用可能性を決定することができる。サーバが管理対象サーバとして定義されている場合、モニタメカニズム 1 3 0 は作動中その利用可能性をモニタすることができる。モニタメカニズム 1 3 0 はサーバから動的負荷共有情報のポーリングを行うことも可能である。サーバがもはや利用できないことをモニタメカニズム 1 3 0 が検出したとき、モニタメカニズム 1 3 0 は、ホスト名を解決する際に A T C メカニズム 1 2 6 が考慮できるように、サーバがもはや利用できないことを示すローカルなポリシーを作成することをデータベース管理者 1 3 2 に知らせることができる。

【 0 0 6 8 】

モニタメカニズム 1 3 0 は、サーバからの動的負荷共有情報のポーリングを行うと、ポーリング済みの負荷共有のダイナミクスにより影響を受けている、ポリシーデータベース 1 2 4 内の負荷共有ポリシーを更新する旨をデータベース管理者 1 3 2 に知らせることができる。例えば、サーバグループ内の 3 つの一次サーバが当初負荷共有（0 . 3、0 . 3、0 . 4）を持っていて、第 3 の一次サーバがその負荷共有を次に 0 . 2 に変更した場合、データベース管理者 1 3 2 は、上記 3 つの一次サーバ間の負荷共有を（0 . 4、0 . 4、0 . 2）へ更新することができる。

【 0 0 6 9 】

レポート作成装置 1 3 4 は、保存されたログ情報 1 3 6 に基づいて基底ネームサーバの処理に関連するレポートを作成する。異なるネームサーバからのレポートを統合できるように、A T C 管理フレームワーク 1 4 2 内のレポートコンソリデータ（c o n s o l i d a t o r）1 5 4 へこのような作成済みレポートを送信することも可能である。

【 0 0 7 0 】

加入者は、2 つの方法、D N S C N A M E または N G 委任のうちの一方の方法で A T C システム（D N S サーバ）を起動（ターンアップ）させることができる。単一の D N S ホスト名を求めてトラフィックを送信するために A T C を使用する代わりに、加入者は、A T C へ向けて送信したい多くの異なるサブドメインを持つことができる。例えば、加入者が、A T C により処理される d l . c u s t o m e r . c o m からのすべてのダウンロードを A T C のサブドメインと共に望むことができ、しかも、d l . c u s t o m e r . c o m により制御される他のすべての領域（w w w . c u s t o m e r . c o m など）を以下の加入者自身のネームサーバにより解決することができる。d l . c u s t o m e r . c o m . = > A T C。a n y . t h i n g . d l . c u s t o m e r . c o m . = > A T C。w w w . c u s t o m e r . c o m . = > A T C でない。c u s t o m e r . c o m . = > A T C でない。

【 0 0 7 1 】

この場合、加入者の D N S ゾーンファイル内に C N A M E レコードを追加する代わりに、加入者は単にそのゾーンファイル内の N S レコードを介して命名を d l . c u s t o m e r . c o m . に委任する。

【 0 0 7 2 】

（N S レコードを利用する）委任方法は、この方法が柔軟性があり、A T C の信頼性と

、スケラビリティと、柔軟性がすべて得られるため、現在好適な方法である。委任のための最初の接触後、時折問合せを行う正しく作動するリゾルバは加入者自身の単複のネームサーバと再び接触しなくなる。この結果、ずっと良好な命名解決パフォーマンスが得られることになる。というのは、加入者のネームサーバを通じて行われる個々の新たなDNS要求をルート指定するという不必要なオーバーヘッドが省かれるからである。CNAME法ではループの中に加入者自身のネームサーバが保持される。すなわち、CNAME TTLが時間切れになるときはいつでも、クライアントリゾルバが加入者のネームサーバへ戻り、レコードをリフレッシュする。

【0073】

CNAME法と委任法の双方の場合、ATCスイッチをターンオフする処理手順は同じであり、加入者がそのDNSゾーンファイルを編集してATCへの委任権限が取り除かれる。DNS要求は、適切な委任に関して時間切れが生じるまで加入者の定義したATCポリシーに基づいてサービスを受け続ける。

【0074】

作動時のシステム：図8(a)はプロセスを示すフローチャートの例であり、この例において、ネームサーバは、本発明の一実施形態によるATCポリシーに基づいてDNS要求を解決する。まず、ユーザはユーザのブラウザ114の中へ(または入力としてURLを受け入れ、クライアント用の対応するリソースを取得する任意のアプリケーションの中へ)URLを入力する(802)。クライアントのリゾルバ116は、サーバのIPアドレスを取得するためにURLのホスト名を解決しようと試みる。上記サーバからURLにより特定されるリソースを取得することができる(804)。クライアントのDNS(図示せず)により、リゾルバ116は、ATCネームサーバネットワーク134内のDNSネームサーバ118へ向けて送信される(806)。リゾルバ116は、解決を試みているホスト名をネームサーバ118に提供する。

【0075】

ネームサーバ118はホスト名の解決要求を受信し(808)、加入者サーバネットワーク104内で、または、リゾルバ116の所在位置に基づいて、並びに、ポリシーデータベース124から検索された関連するATCポリシーに基づいて、クライアントの要求を処理することができるCDN105内で1以上のサーバを確定する(810)。図8(b)と関連してこの処理の詳細について説明する。選択されたサーバのIPアドレスは要求元リゾルバ116へ返信される(812)。次いで、ブラウザ114は、要求したリソースを取得するためにサーバのうちの1つと接続する(814)。

【0076】

図8(b)は、ドメインネームサーバが、クライアントと関連するATCポリシーの位置に基づいて1以上のサーバを選択する典型的処理を示すフローチャートである。リゾルバ116またはクライアントの所在位置をまず決定する(816)。次いで、ポリシーデータベース124から、関連するATCポリシーの検索を行う(818)。クライアントの所定位置と、関連するATCポリシーとに基づいて加入者サーバネットワーク104内のまたはCDN105内のいずれかの1以上のサーバを選択する(820)。

【0077】

図8(c)は、ドメインネームサーバ内のモニタメカニズム130が、加入者サーバネットワーク104内またはCDN105内の、ネームサーバ並びに1以上のサーバの処理をモニタする典型的処理を示すフローチャートである。ドメインネームサービス中に生じるイベントをモニタする(822)。ATCネットワークモニタメカニズム152へ上記のようなイベントを送信する(824)。さらに、1以上のサーバの利用可能性もモニタする(826)。さらに、1以上のサーバのいずれかが管理対象サーバとして定義されていれば(828で判定)、動的負荷共有情報のポーリングを行う(830)。利用可能性情報と動的負荷共有情報(そのような情報が何か存在すれば)の双方を用いて、ネームサーバにとってローカルな何らかのATCポリシーを更新する(832)。

【0078】

図8(d)は、ATCポリシー管理メカニズム152がATCポリシーを動的に維持し、これを配信する典型的処理を示すフローチャートである。最初、異なるソースからポリシーを受信し(834)、ネームサーバ118へこのポリシーを配信する(836)。バックアップが必要であれば(838で判定)、ATCポリシー管理メカニズム152がマスタバックアップエージェント146へ現在のポリシーを送信する(840)。

【0079】

ATCポリシー管理メカニズム152は動的ポリシーの保守管理も行う。ATCポリシー管理メカニズム152は、或る定義した間隔で動的ポリシー情報(842)のポーリングを行い、このようなポーリング済みの動的ポリシー情報を用いて、既存のポリシーを更新する(844)。次いで、更新済みポリシーをネームサーバへ配信する(846)。バックアップエージェントへ更新済みポリシーを伝播する必要があるれば(848で判定)、これらの更新済みポリシーをマスタバックアップエージェントへ送信する(850)。

【0080】

図8(e)は、ATCネットワークモニタメカニズム150がネームサーバの作動をモニタし、NOC148と加入者102とへ警告を送信する典型的処理を示すフローチャートである。異なるネームサーバのモニタメカニズムから送信されたイベントをトラップする(852)。異なるソースからの上記のようなトラップしたイベントを統合し(854)、次いで、処理する(856)。何らかの警告状況が生じた場合(858で判定)、ATCネットワークモニタメカニズム150が警告を作成する(860)。次いで、作成された警告をNOC148と加入者102の双方へ送信する(862)。

【0081】

ポリシー管理：ATCポリシーを最初に設定し、その後、サーバの動的状態に基づいて適宜このポリシーを更新することができる。ATCポリシーは様々な手段を介して形成することができる。上記説明したアプローチを適用して別のポリシーを形成することも可能である。GUIによるアプローチまたはファイルベースのアプローチ(またはこれら双方)を用いて加入者ポリシーを設定することも可能である。GUIによるアプローチによって、加入者ポリシーを形成する異なる手段を採用することも可能である。例えば、ブラウザを用いて直接ポリシーを入力できるようにすることも可能である。GUIによるアプローチを用いて、加入者ポリシーについての説明を含むXMLファイルのロードを行って、ポリシーの構文解析と記憶とを行うことができるようにすることも可能である。別の代替方法として、加入者ポリシーについての説明を含むファイルのロードを同様の方法で行って、適宜構文解析を行うようにすることも可能である。ファイルベースの方法を用いる場合、加入者ポリシー(XMLに基づいて構築された加入者ポリシーか、別の何らかの構造の加入者ポリシーかのいずれか)についての説明を含むファイルにFTPなどの別の手段を介してアクセスすることができる。

【0082】

推奨実施例によっては、加入者が機密保護を施したウェブベースのGUI160(図6)にアクセスして加入者の機密保護を施したブラウザインタフェース156を使用するものもある。

【0083】

図9(a)~9(c)は、本発明の種々の実施形態による、例示の機密保護を施したウェブベースのグラフィカルインタフェースを示し、このインタフェースを介して、加入者は、指定したネットワーク資源と関連して、負荷共有ポリシーとオーバーフローポリシーとを定義することができる。異なるタイプの負荷共有サーバ：(1)静的サーバ、(2)動的サーバ、(3)オーバーフローサーバを設けることができる。動的サーバとは、モニタ対象サーバまたは管理対象サーバのいずれかであり、このサーバの動的利用可能性をモニタすることが可能であり、さらに、サーバが利用できなくなった場合、サーバの負荷を再送信することが可能である。モニタ対象サーバの場合、その負荷共有と負荷分散部分の双方を動的なサーバにすることも可能である。

【0084】

同様に、異なるタイプのサーバへのルート指定要求を決定するポリシーを適宜定義することも可能である。第1に、サーバが比較的静的で、時間中頻繁に変化しなければ、静的サーバを決定するポリシーが適用される。これは、サーバの利用可能性が安定したものであり、異なるサーバ間での負荷共有も比較的安定していることを意味する。サーバが頻繁に変化すると予想される場合、動的サーバを制御するポリシーが適用される。このようなポリシーには、フェイルオーバーポリシー、分散ポリシー、および（前述の）層化フェイルオーバーポリシーが含まれる。オーバーフローポリシーは、静的サーバまたは動的サーバのいずれかの一次サーバが何らかの理由のために利用できなくなったり、過負荷状態になったりしたときの要求フローの変更を制御する。この場合、関連するオーバーフローポリシーによって、どのオーバーフローサーバへネームサービス要求を向けるべきであるかが決定される。

【0085】

所定のサーバと関連する負荷共有とは、静的サーバ設定内の該サーバへ送信されるトラフィック量を表す。サーバへ送信するトラフィックの負荷共有を計算する例示の方法として、現在の静的サーバ設定のすべてのサーバの負荷共有量を加算し、この加算した合計で該サーバの負荷共有を除して、負荷共有を導き出す方法がある。

【0086】

所定のサーバの分散部分は、サーバから再送信すべきトラフィックの割合（％）を表す。負荷共有ポリシーに基づいて負荷共有を行った後、再送信を行うことができる。図9（a）は、個々のリストされたサーバに様々な選択関連パラメータを割り当てたインタフェース例を示す図である。例えば、個々のサーバに対してTTLが指定される。さらに、負荷共有と分散部分とを指定することも可能である。例えば、ニューヨークとロンドンのサーバの双方は1.0の負荷共有を有する。サーバ・ニューヨークに割り当てられた分散部分は0.2であり、これはその負荷の20％が別のあるサーバへ再送信されることを意味し、また、サーバ・ロンドンに割り当てられた分散部分は0.3であり、これはその負荷の30％が別のあるサーバへ再送信されることを意味する。

【0087】

分散部分はリアルタイムで自動的に計算することができる。例えば、サーバの応答が緩慢で、過負荷状態になっている可能性が検出されると、その予想応答時間と実際の応答時間との間の不一致に基づいて分散部分の計算を行うことができる。次いで、自動的に計算されたこのようなトラフィック量を適用し、新しく計算した部分を異なるサーバへ再送信して、当初過負荷状態のサーバへの再送信を意図していたトラフィックの若干の負荷を受け持つようにすることが可能である。

【0088】

個々のリソースサーバの場合、オンラインフラグをセットして、サーバが現在利用可能かどうかを示すことができる。このフラグは図9（a）の右側の列に示されている。このフラグがあると、保守管理などのためにサーバを落す必要がある場合、一時的にサーバの解除を行うことが可能となる。

【0089】

動的サーバの比較的頻繁な変更が予想されるという事実に起因して、動的サーバの選択を決定するポリシーを2段階で定義することができる。静的サーバ用の場合と同様の方法で動的サーバ用のポリシーを当初指定してもよい。例えば、図9（a）に図示のように、ニューヨークとロンドンの動的サーバ用として負荷共有と分散部分とを定義することができる。しかし、作動中、動的サーバの選択を決定するポリシーを動的に確立することも可能である。例えば、ネットワーク上の1以上の指定した位置などから検索したオンライン状態レポートに基づいて、当初定義したポリシー（負荷共有、分散部分、オンラインフラグなど）を適宜改訂することも可能である。ネットワークの健康状態や他の任意のネットワークのパフォーマンスに関連するファクタ（保守管理など）に対して適応的に選択を実行する方法におけるかなりの柔軟性が動的ポリシーによって得られる。

【0090】

加入者が指定した1以上のネットワーク位置のオンライン状態レポートを提供することができる。これらの位置はユニフォームリソースロケータ（URL）として指定することも可能であり、また、HTTP要求を通じて上記位置にアクセスすることも可能である。最初のポリシーで状態レポートの位置を指定して、この位置との一定のリンクを設けることができる。図9（b）は状態レポートとのURLリンクを指定するための例示のGUIを示す。状態レポートの所在位置に関連するURLリンクは"http://server"として指定され、このリンクは10.0.0.3というIPアドレスを持つロンドンと命名されたサーバに対応するものである。このアクセスを認証することも可能であり、このような認証要件は最初のポリシーで指定してもよい。サーバのパフォーマンスのモニタ中に収集した情報に基づいてオンラインアクセス状態レポートを構築することも可能である。例えば、加入者サーバネットワーク内の個々のサーバは、そのパフォーマンスに関連する情報を含む状態レポートを提供することも可能である。ATCネームサーバネットワーク内のネームサーバはこのようなサーバからこのような情報のポーリングを行うことも可能であり、さらに、このような情報を用いてポリシーの更新を行うことができる。

#### 【0091】

状態レポートにアクセスする頻度を明白に指定することも可能である。例えば、30秒毎などの定期的な時刻に状態レポートのポーリングを行うには、上記頻度は関連するメカニズム（具体的には個々のネームサーバのATCポリシー管理メカニズムまたはモニタメカニズム）を必要とする場合もある。

#### 【0092】

拡張可能マークアップ言語（XML）などの何らかの標準的言語を用いて状態レポートを構築することができる。このような状態レポートは改訂されたポリシーを含むことができる。加入者がネットワークパフォーマンスに基づいてこの改訂されたポリシーを手動で決定したり、ネットワークパフォーマンスに基づいて自動化処理によりこのポリシーを接続したり、あるいは、個々の管理対象サーバによりこのポリシーを作成したりすることも可能である。このようなケースで、更新済みポリシーが状態レポートの中に含まれ、この状態レポートのポーリングが行われるとき、以降のトラフィック制御時にこの更新済みポリシーが使用される。例えば、管理対象サーバはその動的容量に基づいてその負荷共有の再定義を行うことができる。このような動的に定義した負荷共有情報にアクセスして、実施時にこの情報を利用するとき、トラフィックはネットワークのダイナミクスに適応して制御される。

#### 【0093】

状態レポートがアクセスされると、関連するメカニズム（ATC管理フレームワーク内のATCポリシー管理メカニズムまたは対応するネームサーバ内のATCメカニズム）は状態レポート内に含まれる情報に基づいて関連するポリシーの更新を行う。例えば、サーバ・ニューヨーク用の現在の負荷共有は、同じ分散部分（0.2）と共に0.4（前回の1.0からダウン）にすることが望ましいこと、また、サーバ・ロンドン用の現在の負荷共有は0.4の分散部分（40%分散部分）と共に0.5（前回の1.0からダウン）にすることが望ましいことを状態レポートによって示すことができる。別のシナリオとして、個々の動的サーバに関するネットワークパフォーマンスデータを提供し、状態レポートにアクセス後、ATCメカニズムが現在のポリシーを適宜改訂することができる方法を状態レポートにより決定してもよい。

#### 【0094】

状態レポートが動的ポリシーを提供する場合、このレポートは一般に、個々の動的サーバに対して、以下の情報を含むことができる：`<ServerStatus loadShare="LS" shedFraction="SF" online="Boolean"/>`。但し、LSとLFは数値を表し、"ブール（Boolean）"は"真"か"偽"かのいずれかの論理値を表す。

#### 【0095】

上述の動的ポリシーのメカニズムの場合、加入者またはサーバは、ATCポリシー階層

全体を更新する必要なく、現行のポリシー（負荷共有、分散部分ポリシー、オンラインフラグなど）に対する変更を簡単に指定することができる。さらに、あるパラメータ（実施形態によっては"ダウンオンライン"と呼ばれる）をA T Cポリシーでセットして、失敗したポーリングや、検索や、状態レポートのコンテンツの構文解析の失敗などの理由に起因して生じる、A T Cポリシー管理メカニズムが状態レポートに正しくアクセスできない状況でA T Cメカニズムの行動を制御することができる。本発明のある実施形態によれば、上記状況の処理に適用できる3つの異なる例示のアプローチがある。

**【0096】**

第1のアプローチとして、加入者は、当該サーバ用の状態レポートを正しく取得できない場合、特定のサーバを選択しないようにネームサーバ内のA T Cメカニズムに指示することができる。加入者は"ダウンオンライン"パラメータを偽にセットすることによりこのポリシーを指定することができる。この場合、A T Cメカニズムは、ポーリングメカニズムが有効な状態レポートを検索するまで、基底サーバを選択処理プロセスの候補とみなさないことになる。

**【0097】**

ポーリングの失敗を処理する第2のアプローチとして、A T Cメカニズムが、そのデフォルトのポリシー（または最初のポリシー）に基づいて基底の動的サーバの選択を可能にするアプローチがある。この解決方法を指定するために、加入者は"ダウンオンライン"パラメータを真にセットすることができる。

**【0098】**

状態レポートを正しく検索できない状況を処理する第3のアプローチとして、基底サーバの"オンライン"フラグがオンであれば（基底サーバが利用可能であれば）A T Cメカニズムが基底サーバを選択できるようにするアプローチがある。これを行うために、加入者は、状態レポートで"オンライン"Server Statusのみを指定し、"ダウンオンライン"は真または偽のいずれかにセットすることができる。この場合、A T Cメカニズムは"オンライン"フラグが真にセットされているとき、ポリシーで指定されている負荷共有と分散部分とを使用する。負荷共有と負荷分散部分とは、双方とも動的に決定することができる（A T Cポリシー管理メカニズムから配信される場合または基底サーバからA T Cメカニズム130によりポーリングされる場合のいずれかの場合）。

**【0099】**

処理上異なるポリシーによりこれらサーバの選択を制御できるが、静的サーバと動的サーバの双方は一次サーバである。第3のタイプのサーバはオーバーフローサーバと呼ばれる。このサーバは、何らかの理由のために一次サーバを選択できない場合、代替サーバを提供するものである。一般に、オーバーフローサーバは、正準名(Canonical name)すなわちCNameに対応し、(ケーブル&無線PLC社のフットプリントサービスなどのような)CDNを提供するサービスを指すものである。オーバーフローサーバの選択は一般に常時利用可能な信頼度に基づいて決定することができる。オーバーフローサーバは図9(c)に示すウィンドウを介して定義することができる。図9(c)で、オーバーフローサーバは、CDNサーバアドレス"customer.footprint.net"(図1に図示のCDN105など)を指すCNameにより定義される。

**【0100】**

図10(a)~図10(b)は、1セットのリソースサーバに基づいて定義された加入者ポリシー例を示す図であり、この加入者ポリシーによって、着信要求の地理上の位置と個々の位置の時間帯などの異なる判断基準に基づいてサーバの選択が決定される。図10(a)では、IPアドレス10.0.0.2を持つ"eastserver"と、IPアドレス10.0.0.1を持つ"westserver"と、CName"customer.footprint.net"を持つサービスネットワークとを含む3つの異なるリソースサーバが定義されている。この場合、サービスネットワークは2以上のサーバを備えたものであってもよい。

**【0101】**

図10(b)は、1セットのサーバへ向けてトラフィックを送信すべき方法を案内する1セットの地理的ポリシーの中に組み込まれた例示の決定ツリーを示す図である。図10(b)に示された決定ツリーでは、アメリカ合衆国と世界の残りの部分との間の分割に基づいて、サーバの選択はまずトップレベルで異なるリソースへ向けられる。リソースは、単一サーバ(またはCDN)あるいは1グループのサーバ(または複数のCDN)のいずれかに対応することができる。アメリカ合衆国以外の地理領域から開始された要求は"ロンドン"と命名されたリソースへ向けて送信される。アメリカ合衆国内では、時間帯ベースのポリシーがさらに適用される。中央時間帯内の領域から開始された要求は"ニューヨーク"と命名されたリソースへ向けて送信される。アラスカ時間帯内の領域から開始された要求はリソース"ロンドン"へ向けて送信される。最後に、これらの時間帯(アラスカまたは中央時間帯)のいずれにも属さないアメリカ合衆国内の領域から開始された要求は"ロンドン"または"ニューヨーク"のいずれかへ向けて送信することができる。

【0102】

図10(c)~図10(d)は、1セットのリソース(サーバまたはCDN)と、オーバーフローポリシーを持つ着信する要求の要求元の地理上の位置に基づいて定義される加入者ポリシーとに基づいて構築される別の決定ツリー例を示す図である。上記オーバーフローポリシーは、一次サーバが利用できなくなった場合、ATCメカニズムが予め定義したオーバーフローサーバへ向けてトラフィックを送信できるようにするポリシーである。図10(c)に図示のリソースウィンドウでは、以下の3つのリソース、すなわちリソースのIPアドレスに基づいて個々に定義された静的リソース"ロンドン"と"ニューヨーク"と、CName"customer.sandpiper.net"を持つ"シドニー"と命名されたサービスネットワークが定義される。個々のリソースは、或る階層を持つサーバグループなどの1セットのサーバに対応するものであってもよい。リソース"ロンドン"はさらに動的リソースと定義され、リソース"シドニー"はさらに"cdn\_service"というニックネームのオーバーフローサーバネットワークとして定義される。図10(d)は、これらのリソースに基づいて構築された決定ツリー例を示す図である。

【0103】

図10(d)の決定ツリーは、要求がアメリカ合衆国からのものかどうかに基づいてまずトップレベルで2つの方向に分かれる。要求がアメリカ合衆国から開始されたものである場合、その要求は、図10(d)に例示のポリシーに基づいてリソース"ロンドン"の第1層にある動的サーバへ向けて送信される。アメリカ合衆国からの要求は、リソース"cdn\_service"内のオーバーフローサーバのうちの1つへ向けても送信することができる。リソース"ロンドン"の第1層にあるすべての一次サーバが機能できなくなった場合、あるいは、このような一次サーバが過負荷状態になった場合に、上記事態が生じる可能性がある。

【0104】

本願明細書に記載の様々なウェブベースのインタフェースの他に、加入者ポリシーを定義できる別の手段も存在する。前述したように、例えば、ATCメカニズムによりダウンロードが可能で、トラフィックの制御に使用できるXMLファイルの形で加入者ポリシーの構築または指定が可能である。

【0105】

異なる手段を介して(ウェブベースのGUIやXMLファイルなどを介して)定義したポリシーを変換して、ATCメカニズム内の何らかの予め定義したフォーマットに変えることも可能である。ATCポリシーの管理と処理時の効率を図るために、このような予め定義したフォーマットを設計することも可能である。例えば、ATCポリシー用の内部形式を設計して、内部でAMAがATCポリシーの記憶と、アクセスと、ネームサーバエージェントへの配信とを都合よく行うことができるように、さらに、ネームサーバエージェントが効率良くポリシーを適用できるようにすることも可能である。

【0106】

前述したように、ATCポリシーの管理に加えて、AMAはネームサーバのパフォーマ

ンスをモニタすることも可能であり、さらに、閲覧可能なDNSログレポートを作成する。モニタメカニズムは、ネームサーバのDNSログまたはネームサーバからトラップされたイベントのいずれからパフォーマンス情報を収集することができる。レポート作成メカニズムによりこのような収集情報を利用して、情報を与えるレポートを構築するようにすることも可能である。このレポート作成メカニズムは加入者が機密保護を施したウェブベースのGUIを介してこのようなレポートを利用できるようにすることも可能である。図11(a)~図11(c)は、機密保護を施したウェブベースのGUIを介してアクセス可能な例示タイプのレポート情報を示す図示である。図11(a)は、加入者が指定のリソースサーバのDNSログデータを閲覧できるようにするウェブインタフェースを示す図である。加入者は現在再査しているサーバの名前("download.subscriber.com"など)と、ログデータを編成すべき形式(IPとCNameの間合せと、出力時の別個の項目としての応答を伴う返答との表示を意味する"別個"の出力スタイルの指定など)と、現在再査している時期(2002年9月1日~2002年9月24日など)と、ログデータの表示時に用いる時間分解能(時間分解能の自動的選択など)とを指定することが可能である。

#### 【0107】

図11(b)は指定サーバと関連するログデータのプロットを示す。このログデータは、或る分解能で、指定された時間(X軸)に対する特定サーバのログエントリに基づいて作成され、プロットで示されている。このプロット例は、2002年9月24日の2:30pm~3:30pmの間の時間中、基底サーバへ向けて送信されたトラフィックの量を反映するものである。トラフィック量は、分当たり基底サーバが生成した返答回数という点から記述される(Y軸)。2:36pmと2:38pmとの間でトラフィックボリュームの急上昇が生じていることがこのプロット例で理解できる。

#### 【0108】

図11(c)は、図11(b)のものと同じログデータの図表を示し、この図表では、表の上部から下部までログデータが時間順にリストされている。例えば、左列の各行は時間をリストしている。例示の表では、1時間(2:30pm~3:30pm)の範囲内のログデータは、各々15分の複数のサブ期間に分けられている。個々のサブ期間の間、第3列は対応するサブ期間からの返答回数を出力する。例えば、3:15pm~3:30pmのサブ期間中、13回の返答があり、別のサブ期間には返信がない(図11(b)に示すプロットと一致)。

#### 【0109】

本願明細書に記載の様々なメカニズムには、限定なしで、適応型トラフィック制御(ATC)メカニズム、所在位置決定メカニズム、ポリシー編集メカニズム、管理ポリシー更新メカニズム、ATCポリシー管理メカニズム、レポート作成メカニズム、モニタメカニズムが含まれ、ハードウェアや、ソフトウェアまたはそれらを組み合わせた形で管理マスタバックアップメカニズムの実現が可能である。ソフトウェアの形で実現する場合、いずれの任意のタイプの適切な解釈またはコンパイルされるプログラム言語で上記メカニズムを実行することができる。ソフトウェアの形で部分的にまたは完全に実現された場合、本発明の態様は、ROM、ディスク、ASIC、PROM、等を含む任意のメモリまたは記憶媒体上に存在することができる(但しこれらに限定されるものではない)。特定のメカニズム(アルゴリズム、処理プロセスおよび機能)並びにアーキテクチャと関連して本発明について説明したが、当業者であれば、本発明をそのまま達成しながら、別のメカニズムおよび/またはアーキテクチャを使用することも可能であることを理解するであろう。

#### 【0110】

本発明の様々なメカニズムが(クライアント側やサーバ側の)特定のマシーンで機能している場合、これらのメカニズムはマシンのメモリ内にまたは記憶装置上にもしくはこれらを組み合わせた形で存在するものであってもよい。さらに、特定の順序で実行するものとして上記処理の多くを示したが、当業者であれば、何らかの並列処理を含む別の順序も可能であり、これも本発明の範囲に属することを理解するであろう。

## 【 0 1 1 1 】

以上、本発明の好ましい実施形態と関連して本発明について記載したが、本記載は専ら例示を目的として行ったものであり、本発明は、本記載により限定されるものではない。実際、本発明の変形例は当業者には容易に明らかなものであろう。このような変形例も本発明の範囲に属するものである。したがって、例示の実施形態と関連して本発明について説明したが、本願明細書に用いた用語は、限定のための用語ではなく説明のための用語である。本発明の範囲と精神から逸脱することなく、添付の請求項の範囲内で変更を行うことが可能である。特定の構造、作用、材料と関連して本願明細書で本発明について記載したが、本発明は開示された上記詳細事項に限定されるものではなく、添付の請求の範囲内ですべての均等な構造、作用、材料に拡張されるものである。

## 【 0 1 1 2 】

上記記載の処理は、正しくプログラムされた汎用コンピュータ単独で実行することも可能であり、あるいは、専用コンピュータと接続して実行することも可能である。このような処理は、単一のプラットフォームにより、あるいは、分散処理用プラットフォームにより実行することも可能である。さらに、専用ハードウェアの形でまたは汎用コンピュータにより実行されるソフトウェアの形でこのような処理と機能とを実現することが可能である。このような処理時に処理されたデータ、または、このような処理の結果形成されたデータは当業で一般的な任意のメモリに記憶することが可能である。例えば、所定のコンピュータシステムやサブシステムの R A M のような一時メモリにこのようなデータを記憶することも可能である。さらに、あるいは、代替の形で、例えば磁気ディスク、書き換え可能な光ディスク、等々の長期間の記憶装置にこのようなデータを記憶することも可能である。本願明細書での開示を目的として、コンピュータ可読媒体は、このような現行のメモリ技術、並びに、このような構造とこのようなデータのハードウェアあるいは回路表現を含むデータ記憶メカニズムを含む任意の形態のデータ記憶装置を含むことも可能である。

## 【 図面の簡単な説明 】

## 【 0 1 1 3 】

【 図 1 】 本発明の種々の実施形態によるフレームワークを示す。

【 図 2 】 本発明の種々の実施形態によるポリシーの例を示す。

【 図 3 】 本発明の種々の実施形態による、加入者ポリシーに基づいて構成される階層または決定ツリーの例を示す。

【 図 4 】 本発明の種々の実施形態による、加入者のネットワーク階層と加入者ポリシー間の関係の例を示す。

【 図 5 】 本発明の種々の実施形態による、適応型トラフィック制御のフレームワークの高レベルのアーキテクチャを示す。

【 図 6 】 本発明の種々の実施形態による、管理マスタエージェント ( A M A ) の高レベル機能ブロック図を示す。

【 図 7 】 本発明の種々の実施形態による、モニタメカニズムの内部機能ブロック図を示す。

【 図 8 ( a ) 】 本発明の種々の実施形態による、コンテンツ配信フレームワークは適応型ポリシーベースのドメインネームサービスを提供するプロセスを示すフローチャートの例である。

【 図 8 ( b ) 】 本発明の種々の実施形態による、ドメインネームサーバがポリシーをベースとするホスト名を解決するプロセスを示すフローチャートの例である。

【 図 8 ( c ) 】 本発明の実施形態による、上記プロセスでドメインネームサーバのモニタメカニズムがネームサービスオペレーション並びにサーバの利用可能性と負荷共有状態とを動的にモニタするあるプロセスを示すフローチャートの例である。

【 図 8 ( d ) 】 本発明の種々の実施形態による、上記プロセスで A T C 管理ネットワークが動的ポリシーを保持し、コンテンツ配信フレームワークの動作をモニタするあるプロセスを示すフローチャートの例である。

【 図 8 ( e ) 】 本発明の種々の実施形態による、 A T C ネットワークモニタメカニズムが

異なるドメインネームサーバからイベントを捕捉し、必要な場合に警告を生成するプロセスを示すフローチャートの例である。

【図9(a)】本発明の種々の実施形態による、例示の機密保護を施したウェブベースのグラフィカルインタフェースを示し、上記インタフェースを介して加入者は静的リソース間の負荷共有と分散部分ポリシーとを定義することができる。

【図9(b)】本発明の種々の実施形態による、動的サーバに対するポリシーを定義するための例示インタフェースを示す。

【図9(c)】本発明の種々の実施形態による、正準名(canonical name)を用いてオーバーフローサーバが定義される例示のグラフィックユーザインタフェースを示す。

【図10(a)】本発明の種々の実施形態による、1セットのリソースサーバに基づいて定義される加入者ポリシー例を示し、この加入者ポリシーにより、着信要求の地理上の位置と、それぞれの位置の時間帯とに基づいて選択が決定される。

【図10(b)】本発明の種々の実施形態による、1セットのリソースサーバに基づいて定義される加入者ポリシー例を示し、この加入者ポリシーにより、着信要求の地理上の位置と、それぞれの位置の時間帯とに基づいて選択が決定される。

【図10(c)】本発明の種々の実施形態による、オーバーフローポリシーにより、一次サーバが利用できなくなった場合、ATCメカニズム150が予め定義したサービス向けにトラフィックを送信することが可能となるオーバーフローポリシーと共に着信要求の地理上の位置に基づいて定義される加入者ポリシーの例を示す。

【図10(d)】本発明の種々の実施形態による、オーバーフローポリシーにより、一次サーバが利用できなくなった場合、ATCメカニズム150が予め定義したサービス向けにトラフィックを送信することが可能となるオーバーフローポリシーと共に着信要求の地理上の位置に基づいて定義される加入者ポリシーの例を示す。

【図11(a)】本発明の種々の実施形態による、グラフィックユーザインタフェースを介してログ情報を表示し、閲覧することが可能な例示のアーカイブされたログ情報を示す。

【図11(b)】本発明の種々の実施形態による、グラフィックユーザインタフェースを介してログ情報を表示し、閲覧することが可能な例示のアーカイブされたログ情報を示す。

【図11(c)】本発明の種々の実施形態による、グラフィックユーザインタフェースを介してログ情報を表示し、閲覧することが可能な例示のアーカイブされたログ情報を示す。