(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-127290
(P2004-127290A)
(43)公開日　平成16年4月22日(2004.4.22)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06F 15/00	G06F 15/00	310D	5B085
G06F 15/00	G06F 15/00	330B	5J104
H04L 9/32	H04L 9/00	673A	

審査請求 有　請求項の数 15　ＯＬ　（全 18 頁）

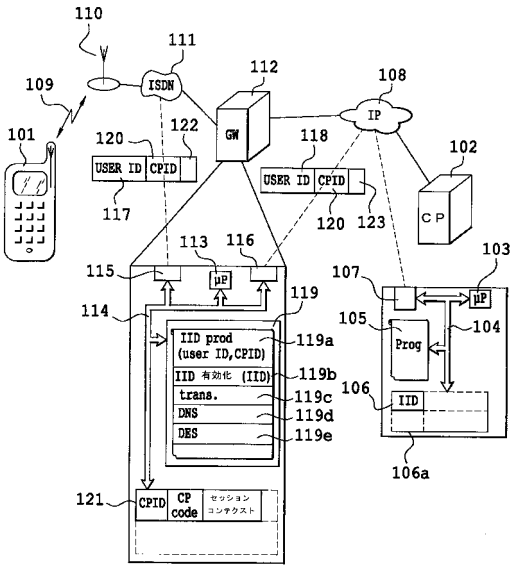
(21)出願番号　特願2003-332294(P2003-332294)
(22)出願日　平成15年9月24日(2003.9.24)
(31)優先権主張番号　0211808
(32)優先日　平成14年9月24日(2002.9.24)
(33)優先権主張国　フランス(FR)

(71)出願人　503347312
ソシエテ　フランセーズ　デュ　ラディオテレフォンヌ
ＳＯＣＩＥＴＥ　ＦＲＡＮＣＡＩＳＥ　ＤＵ　ＲＡＤＩＯＴＥＬＥＰＨＯＮＥ
フランス共和国，９２９１５　パリ　ラ　デファンス　セデックス，プラス　キャルポー，１，トゥール　セコイア
(74)代理人　100080447
弁理士　太田　恵一
(72)発明者　ジャン－フィリップ，ヴァリー
フランス共和国，９２３４０　ブール　ラ　レーヌ，リュ　ドゥ　ラ　フォンテーヌ　グルロ，４１，バティマン　４

Ｆターム(参考)　5B085 AE01 AE09
5J104 AA07 KA01 KA04 NA05 PA07

(54)【発明の名称】データ通信ネットワークに接続するユーザーを分離する第一識別子の作成方法

(57)【要約】
【課題】　ユーザーがアクセスプロバイダを介してコンテンツプロバイダにアクセスする際に、ユーザーのプライバシーを保護できるような、コンテクスト識別子の作成方法を提供する。
【解決手段】第一のコンテクスト識別子は、テレマティクスネットワークと、アクセスプロバイダによってユーザーが自由に使える手段とを介してコンテンツプロバイダに接続するユーザーを分離し、アクセスプロバイダによる第二の識別子（１１７）は、ユーザーの識別を行い、アクセスプロバイダの手段が、第一のコンテクスト分離識別子を第二の識別子に結びつけるためのゲートウェイ（１１２）を有し、第一のコンテクスト分離識別子を作成するために、第一のコンテクスト分離識別子とユーザーとの間の結びつきを確保するための第一のフィールド（２０１）を有し、第一のコンテクスト分離識別子を作成するために、コンテンツプロバイダに応じて第一の識別子の可変性を確保するための第二のフィールド（２０２）を用い、第一と第二のフィールドがコード変換される。



【特許請求の範囲】
【請求項１】
テレマティクスネットワークと、アクセスプロバイダによってユーザーが自由に使える手段とを介してコンテンツプロバイダに接続するユーザーを分離する第一のコンテクスト識別子を作成する方法であり、ユーザーの識別はアクセスプロバイダによる第二の識別子で行われるものであって、
・アクセスプロバイダの手段が、第一のコンテクスト分離識別子を第二の識別子に結びつけるためのゲートウェイを有し、
・第一のコンテクスト分離識別子を作成するために、第一のコンテクスト分離識別子とユーザーとの間の結びつきを確保するための第一のフィールドを有し、
・第一のコンテクスト分離識別子を作成するために、コンテンツプロバイダに応じて第一の識別子の可変性を確保するための第二のフィールドが必要であり、
・第一と第二のフィールドがコード変換されることを特徴とする、作成方法。
【請求項２】
第一のフィールドが第二の識別子を有することを特徴とする、請求項１に記載の方法。
【請求項３】
ユーザーとアクセスプロバイダとの間に存在する契約によって、第二のフィールドの内容が決まることを特徴とする、請求項１または２のいずれか一つに記載の方法。
【請求項４】
コンテクスト分離識別子の有効期間の管理が第二のフィールドの内容によって行われ、その内容は一定の頻度で変わり、その頻度がコンテクスト識別子の有効期間の頻度となることを特徴とする、請求項１から３のいずれか一つに記載の方法。
【請求項５】
コンテクスト識別子の有効期間の管理がコード変換を実行するために用いられるキーによって行われ、そのコード変換は所定の頻度で変わり、その頻度がコンテクスト識別子の有効期間の頻度となることを特徴とする、請求項１から３のいずれか一つに記載の方法。
【請求項６】
第一の識別子が、識別子の種類を含む第三のフィールドを有することを特徴とする、請求項１から５のいずれか一つに記載の方法。
【請求項７】
第一の識別子が、アクセスプロバイダを識別するための第四のフィールドを有することを特徴とする、請求項１から６のいずれか一つに記載の方法。
【請求項８】
第三及び第四のフィールドが暗号化されていないことを特徴とする、請求項６または７に記載の方法。
【請求項９】
第一のフィールドが、ユーザーをアクセスプロバイダに結びつける契約の識別子を有することを特徴とする、請求項１から８のいずれか一つに記載の方法。
【請求項１０】
コンテクスト識別子が普遍的であり、また、同一のコンテクスト識別子により、ユーザーは同一のコンテンツプロバイダの様々なタイプのサーバーに接続できることを特徴とする、請求項１から９のいずれか一つに記載の方法。
【請求項１１】
第二のフィールドの内容が疑似乱数データであることを特徴とする、前記請求項１から１０のいずれか一つに記載の方法。
【請求項１２】
疑似乱数データが日付であることを特徴とする、前記請求項１１に記載の方法。
【請求項１３】
ゲートウェイに関しては、ランダムエレメントが、予め定められた期間において一定であることを特徴とする、請求項１１に記載の方法。

【請求項１４】
第一と第二のフィールドをコード変換するための暗号化方法が、ブロックごとの対称的暗号化方法であることを特徴とする、請求項１から１３のいずれか一つに記載の方法。
【請求項１５】
第一と第二のフィールドをコード変換するための暗号化方法が、ブロック連鎖を用いる対称的暗号化方法であることを特徴とする、請求項１から１３のいずれか一つに記載の方法。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明が対象とするのは、テレマティクスネットワークに接続するユーザーを分離する第一の識別子を作成する方法である。
本発明の分野は、ユーザーがアクセスプロバイダを介してコンテンツプロバイダにアクセスすることに関する分野である。
本発明の分野は、特に、携帯電話ネットワークと、インターネット・タイプのネットワーク、音声、ＳＭＳ、ＭＭＳ、あるいはその他のマルチメディアまたはモノメディアのコンテンツ伝送媒体との間に存在するゲートウェイに関する分野である。
【０００２】
本発明の一つの目的は、ユーザーのプライバシーを保護することである。
【０００３】
本発明のもう一つの目的は、ネットワーク上のアクターが持つクライアントデータベースを保護し、行動分析活動を制限することである。
【０００４】
本発明のもう一つの目的は、通信の秘密保持に寄与することである。
【０００５】
本発明のもう一つの目的は、認可を受けた法人がユーザーを民事的に識別することができるようにすることである。
【０００６】
本発明のもう一つの目的は、コンテンツプロバイダが、前記コンテンツプロバイダに接続するユーザーについて一つまたは複数のコンテクストを管理できるようにすることである。
【背景技術】
【０００７】
現行技術においては、コンテンツプロバイダが、自らのサービスの一つにアクセスするユーザーを識別する手段は幾つも存在している。
それらの手段は、ユーザーがサービスにアクセスするのにどのようなメディアを用いるかによって左右される。
主に四つのアクセス・モードが区別されるが、それで全てが網羅されているわけではない。
第一のアクセス・モードは、インターネット・タイプのアクセスである。
インターネット・モードは、それ自体が、接続モードと非接続モードと呼ばれる、二つのサブ・モードに更に小分けされる。
接続インターネット・モードとは、ＨＴＴＰまたはＷＴＰ（Ｗｉｒｅｌｅｓｓ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ、すなわち、無線伝送プロトコル）タイプのプロトコルを用いる接続モードである。
例えばＨＴＴＰサーバーとは、例えばインターネットのネットワークを介して、ＨＴＴＰプロトコルにより通信を行う機器である。
そのようなサーバーが、ＷＥＢサイトやＷＡＰ（つまり携帯電話に適合させたインターネットの）サイトのホストとなる。

また、ＳＭＴＰタイプのプロトコルを介した非接続インターネット・アクセス・モードも存在するのであり、そのようなモードにおいて接続とは、実際には、メールタイプの電子メッセージを交換することにある。

【０００８】

もう一つのアクセス・モードは、オペレーターによるアクセス・モードであり、それもまた二つのサブ・モードに小分けされる。

その場合、第一のサブ・アクセス・モードは、ＳＭＳ（Ｓｈｏｒｔ　Ｍｅｓｓａｇｅ　Ｓｅｒｖｉｃｅ）またはＭＭＳ（Ｍｕｌｔｉｍｅｄｉａ　Ｍｅｓｓａｇｅ　Ｓｅｒｖｉｃｅ）タイプのプロトコルを介した、非接続型と呼べるようなアクセス・モードであり、該サブ・アクセス・モードは、全体として四つのアクセス・モードのうちの三つめのアクセス・モードを構成する。

第四のアクセス・モードは、音声モードとも呼ばれる、オペレーターによる接続モードであり、そのモードにおいては、ユーザーは音声サーバーに接続してアクセスする。

【発明の開示】

【発明が解決しようとする課題】

【０００９】

それら四つのアクセス・モードに関しては、単純なタイプの解決策があり、それは、サーバーに接続する際に、識別子とパスワードの入力を申し出るようなインターフェイスを実現するということである。

コンテンツプロバイダのサーバーに接続しているユーザーが携帯電話を介してそれを行う限りにおいて、ユーザーが識別子（すなわちログイン）とパスワードを入力するために使える手段は、電話のユーザー・インターフェイスによって限定されることになる。

識別子とパスワードが全て数字である場合には、記憶するのは困難で、当てるのは簡単である。

識別子とパスワードが英数字の場合には、ボタンが九つしかないキーパッドでそれらを入力するのは面倒である。

更に、この入力の手順はユーザーにとって余計な手間ということになり、その結果、大抵の場合、携帯電話のユーザーは、識別子とパスワードのタイプの接続インターフェイスを申し出るようなサイトに接続するのを思いとどまることになる。

【００１０】

もう一つの解決法は、第一のタイプのサーバーの場合のもので、クッキーを利用することである。

クッキーというのは、ユーザーの機器に記録された小さなファイルである。

コンテンツプロバイダへの接続の際には、コンテンツプロバイダはそのクッキーにアクセスすることによりユーザーを識別することができる。

この解決法の問題は、電子的な方法などでクッキーを盗むことが可能だというところにある。

それゆえに、クッキーを使うことは、セキュリティに対する高い要求とは両立できないことになる。

その場合のもう一つの問題は、クッキーは比較的に評判が悪く、そのため、ユーザーがクッキーを削除したがるということである。

更に、ユーザーは、コンテンツプロバイダに接続するのに使用するアプリケーションやナビゲーターを、そのようなアプリケーションがクッキーを受け付けないように設定することができる。

そのような場合には、ユーザーはコンテンツプロバイダのサーバーに接続するのが不可能になる。

【００１１】

第三と第四のアクセス・モードについては、大抵の場合、コンテンツプロバイダはサーバーにアクセスする人の電話番号を知ることができる。

それゆえ、コンテンツプロバイダは、その電話番号を介して人物を識別することができ

る。
これは、必然的にプライバシーを保護する上で問題となる。
実際、コンテンツプロバイダのサーバーに接続する際に、自分が物理的に識別されてしまうことを望まないというユーザーの希望は、まったく正当なのである。
実際、匿名で利益を得ることが可能でなければならない。
その場合には自分の番号を隠して接続を試みることも可能なのであるが、その場合には、サービスの料金を請求することが不可能であり、従って、有効な接続を行うことができない。
そういうわけで、現時点では、唯一の解決法は、そのコンテンツプロバイダに接続しないということである。

【００１２】
本文の説明において、また実際においても、コンテンツプロバイダにアクセスするということは、コンテンツプロバイダのサーバーに接続するということに等しい。
【課題を解決するための手段】
【００１３】
本発明は、ユーザーがコンテンツプロバイダに提示する識別子を作成できるようにすることでこれらの問題を解決するのであって、この識別子とは、その識別子を作成した本人以外は、ユーザーを民事的に識別することができないようなものである。
そのような識別子により、ユーザーのプライバシーは確かに保護され、ユーザーを識別することを望み、かつ、識別子並びにその識別子が作成された日付を有している管理者が作成したリクエストを介して、そのような識別子によってユーザーを識別することが確かに可能である。
【００１４】
本発明による識別子は、それを作成するためのフィールドが少なくとも二つ必要である。
第一のフィールドはユーザーの識別子で、第二のフィールドは分離識別子の可変性の確保を可能にするフィールドである。
この可変性の確保は疑似乱数によって、あるいは、ユーザーが表明する意思によって行われる。
その場合、第一と第二のフィールドは組み合わされて、コード変換され、それにより、第一のフィールドに誰もアクセスできないようにする。
アクセスプロバイダだけが、つまり、分離識別子を作成するエンティティだけが、その暗号を逆に辿る能力、したがって、ユーザーを民事的に識別する能力を有するのである。れる。
本発明が追求する目的は、そのようにして確かに達成される。
【００１５】
そういうわけで、本発明が対象とするのは、テレマティクスネットワークと、アクセスプロバイダ（１１２）によってユーザーが自由に使える手段とを介してコンテンツプロバイダに接続するユーザーを分離する第一のコンテクスト識別子（１１８、２００）を作成する方法であり、ユーザーの識別はアクセスプロバイダによる第二の識別子（１１７）で行われるものであって、
・アクセスプロバイダの手段が、第一のコンテクスト分離識別子を第二の識別子に結びつけるためのゲートウェイ（１１２）を有し、
・第一のコンテクスト分離識別子を作成するために、第一のコンテクスト分離識別子とユーザーとの間の結びつきを確保するための第一のフィールド（２０１）が少なくとも一つ必要であり、
・第一のコンテクスト分離識別子を作成するために、コンテンツプロバイダに応じて第一の識別子の可変性を確保するための第二のフィールド（２０２）が必要であり、
・第一と第二のフィールドがコード変換されること、を特徴としている。
【００１６】

すなわち、本発明の課題を解決するための手段は、次のとおりである。
第１に、テレマティクスネットワークと、アクセスプロバイダ（１１２）によってユーザーが自由に使える手段とを介してコンテンツプロバイダに接続するユーザーを分離する第一のコンテクスト識別子（１１８、２００）を作成する方法であり、ユーザーの識別はアクセスプロバイダによる第二の識別子（１１７）で行われるものであって、
・アクセスプロバイダの手段が、第一のコンテクスト分離識別子を第二の識別子に結びつけるためのゲートウェイ（１１２）を有し、
・第一のコンテクスト分離識別子を作成するために、第一のコンテクスト分離識別子とユーザーとの間の結びつきを確保するための第一のフィールド（２０１）を有し、
・第一のコンテクスト分離識別子を作成するために、コンテンツプロバイダに応じて第一の識別子の可変性を確保するための第二のフィールド（２０２）が必要であり、
・第一と第二のフィールドがコード変換されることを特徴とする、作成方法。
第２に、第一のフィールドが第二の識別子を有することを特徴とする、上記第１に記載の方法。
第３に、ユーザーとアクセスプロバイダ（３０２－３０５）との間に存在する契約によって、第二のフィールドの内容が決まることを特徴とする、上記第１または第２のいずれか一つに記載の方法。
第４に、コンテクスト分離識別子の有効期間の管理が第二のフィールド（２０２）の内容によって行われ、その内容は一定の頻度で変わり、その頻度がコンテクスト識別子の有効期間の頻度となることを特徴とする、上記第１から第３のいずれか一つに記載の方法。
第５に、コンテクスト識別子の有効期間の管理がコード変換を実行するために用いられるキーによって行われ、そのコード変換は所定の頻度で変わり、その頻度がコンテクスト識別子の有効期間の頻度となることを特徴とする、上記第１から第３のいずれか一つに記載の方法。
第６に、第一の識別子が、識別子の種類を含む第三のフィールド（２０４）を有することを特徴とする、上記第１から第５のいずれか一つに記載の方法。
第７に、第一の識別子が、アクセスプロバイダを識別するための第四のフィールド（２０３）を有することを特徴とする、上記第１から第６のいずれか一つに記載の方法。
第８に、第三及び第四のフィールドが暗号化されていないことを特徴とする、上記第６または第７のいずれか一つに記載の方法。
第９に、第一のフィールドが、ユーザーをアクセスプロバイダに結びつける契約の識別子（２０５）を有することを特徴とする、上記第１から第８のいずれか一つに記載の方法。
第１０に、コンテクスト識別子が普遍的であり、また、同一のコンテクスト識別子により、ユーザーは同一のコンテンツプロバイダの様々なタイプのサーバーに接続できることを特徴とする、上記第１から第９のいずれか一つに記載の方法。
第１１に、第二のフィールドの内容が疑似乱数データ（３０３）であることを特徴とする、上記第１から第１０のいずれか一つに記載の方法。
第１２に、疑似乱数データが日付であることを特徴とする、上記第１１に記載の方法。
第１３に、ゲートウェイに関しては、ランダムエレメントが、予め定められた期間において一定であることを特徴とする、上記第１１に記載の方法。
第１４に、第一と第二のフィールドをコード変換するための暗号化方法が、ブロックごとの対称的暗号化方法であることを特徴とする、上記第１から第１３のいずれか一つに記載の方法。
第１５に、第一と第二のフィールドをコード変換するための暗号化方法が、ブロック連鎖を用いる対称的暗号化方法であることを特徴とする、上記第１から第１３のいずれか一つに記載の方法。

【発明の効果】

【００１７】

本発明の効果は、次のとおりである。

ユーザーのプライバシーを保護することができる。
ネットワーク上のアクターが持つクライアントデータベースを保護し、行動分析活動を制限することができる。
通信の秘密保持に寄与することができる。
認可を受けた法人がユーザーを民事的に識別することができるようにすることができる。
コンテンツプロバイダが、前記コンテンツプロバイダに接続するユーザーについて一つまたは複数のコンテクストを管理できるようにすることができる。

【発明を実施するための最良の形態】

【００１８】

本発明は、以下の説明を読み、添付図面を検証することにより更によく理解されていく。
それら図面は、例示としてのみ示されるのであって、本発明を限定する趣旨のものでは全くない。

・図１は本発明の方法を実施するために有用な手段を示す概略図である。
・図２は本発明の分離識別子の構造の概略図である。
・図３は本発明の方法を実施する手順の概略図である。

【００１９】

図１に示される通信機器１０１は、ユーザーがコンテンツプロバイダのサーバー１０２に接続するために用いるものである。
実際には、通信機器１０１は、種々様々なプロトコルによって通信を確立することのできる携帯電話である。
これらのプロトコルの中でも、インターネット、音声そしてＳＭＳプロトコルと互換性のあるプロトコルを挙げることができる。
言い換えれば、通信機器１０１は、例えば、携帯電話であり、ＷＡＰモードで、音声モードで、そして／またはＳＭＳモードで通信を確立することができるものである。

【００２０】

コンテンツプロバイダのサーバー１０２は、通信機器１０１について既に挙げたプロトコルの少なくとも一つにより通信することができるものである。
コンテンツプロバイダのサーバー１０２が有するマイクロプロセッサー１０３は、サーバー１０２の内部のバス１０４に接続されている。
バス１０４によって、マイクロプロセッサーをプログラム・メモリー１０５と、ユーザー・メモリー１０６、そしてインターフェイス回路１０７と、例えばインターネット１０８によって接続できる。

【００２１】

プログラム・メモリー１０５が有するインストラクション・コードは、様々な機能を実行する際にマイクロプロセッサーを制御するものである。
特にプログラム・メモリー１０５は、既に挙げたプロトコルの少なくとも一つを利用するためのインストラクション・コードを有する。

【００２２】

ユーザー・メモリー１０６は、例えば、データベースに関するものである。
そのため、ユーザー・メモリー１０６は、少なくともユーザーがコンテンツプロバイダのサーバー１０２に接続する可能性のあるだけの数、または、既に接続されているだけの数の行を有する表として記載されている。
各行は、ある数のフィールドを有する。
列１０６ａは、ユーザーを識別するフィールドに対応している。
そこに関わるのが本発明の識別子である。
コンテンツプロバイダのサーバー１０２がリクエストを受信する際には、そのリクエストがこの識別子を有する。
これによってコンテンツプロバイダのサーバー１０２は、ユーザーを識別することがで

き、例えばそのユーザーの好みを特定することができる。
そのような好みの集合をコンテクストという。
一つのコンテクストが有する様々な情報により、ユーザーは、ユーザーが接続したサーバーが提示する外観および／またはコンテンツ、情報を自分の好みにあったものにすることができる。
【００２３】
本例において、ユーザー・メモリー１０６は、コンテンツプロバイダのサーバー１０２の中に含まれている。
実際には、このデータベースに関するユーザー・メモリー１０６のホストになるのは、コンテンツプロバイダのサーバー１０２が接続して前記データベースのコンテンツにアクセスすることのできる他のサーバーでもよい。
【００２４】
ユーザーが通信機器１０１を使ってコンテンツプロバイダのサーバー１０２に接続する際には、携帯電話である通信機器１０１が基地局１１０との間に無線接続１０９を確立する。
基地局１１０は、それ自体が、例えばＩＳＤＮネットワーク１１１を介して、例えば携帯電話である通信機器１０１のユーザーが加入しているアクセスプロバイダのゲートウェイ１１２に接続されている。
ＩＳＤＮネットワーク１１１は、実際には、交換電話ネットワークの全部または一部である。
実際上は、ＩＳＤＮネットワーク１１１は、基地局をアクセスプロバイダのゲートウェイ１１２に接続することのできる技術的解決法であれば何でもよい。
アクセスプロバイダは、例えば携帯電話のオペレーターである。
【００２５】
コンテンツプロバイダは、例えば、インターネット・ポータルという名でも知られているインターネットへのアクセス・ゲートウェイであり、天気予報の音声サーバーであり、標準ＳＭＳサーバーである。
【００２６】
アクセスプロバイダのゲートウェイ１１２が有するマイクロプロセッサー１１３は、バス１１４に接続されている。
このバス１１４には、ＩＳＤＮネットワーク１１１とのインターフェイス回路１１５および、インターネット１０８とのインターフェイス回路１１６も接続されている。
それゆえ、アクセスプロバイダのゲートウェイ１１２はＩＳＤＮネットワーク１１１とインターネット１０８との間のゲートウェイである。
【００２７】
ＩＳＤＮネットワーク１１１においては、通信機器１０１と、その機器のユーザーの識別は、ユーザーの識別子１１７によって行われる。
インターネット１０８においては、通信機器１０１のユーザーの識別は、分離識別子１１８によって行われる。
アクセスプロバイダのゲートウェイ１１２の役割は、ユーザーの識別子１１７と分離識別子１１８との間の連絡を確立することである。
アクセスプロバイダのゲートウェイ１１２のもう一つの役割は、従来のように、ＩＳＤＮネットワーク１１１で使用されているプロトコルとインターネット１０８で使用されているプロトコルとの間でプロトコルの変換を確実に行うことである。
ユーザーの識別子１１７は、例えば、通信機器１０１のユーザーの電話番号である。
このような識別子１１７は、公開の識別子であり、それにより、誰でも、その識別子１１７と物理的な人物とを結びつけられるようなものである。
そのような公開の識別子は、例えば、電話番号、Ｅメール・アドレス、公開インターネット・アドレス等である。
本発明の目的の一つは、コンテンツプロバイダが、コンテンツプロバイダのサーバー１

０２に接続する人物を物理的に、すなわち民事的に、識別できないようにすることである。

【００２８】

アクセスプロバイダのゲートウェイ１１２は、プログラム・メモリー１１９を有している。

プログラム・メモリー１１９が有する様々な区域は、マイクロプロセッサー１１３が実行するタスクにそれぞれ対応するようなインストラクション・コードを有している。

【００２９】

プログラム・メモリー１１９の区域の中で、はっきりと区別できる区域ａ１１９ａはインストラクション・コードを有している。

該インストラクション・コードは、分離識別子１１８の作成に対応しているのであるが、この作成は、アクセスプロバイダのゲートウェイ１１２、つまり、実際にはマイクロプロセッサー１１３によって、少なくともユーザーの識別子１１７に基づき、そしてより望ましい実施様態においてはコンテンツプロバイダの識別子１２０に基づいて行われる。

【００３０】

区域ｂ１１９ｂが有するインストラクション・コードにより、アクセスプロバイダのゲートウェイ１１２がコンテンツプロバイダのサーバー１０２からのリクエストを受信したときに、アクセスプロバイダのゲートウェイ１１２は分離識別子１１８を有効化することができる。

区域ｃ１１９ｃが有するインストラクション・コードにより、アクセスプロバイダのゲートウェイ１１２は分離識別子１１８に基づいてユーザーを識別することができる。

それは、例えばコンテンツプロバイダのサーバー１０２の応答を通信機器１０１に伝送するために用いられるものである。

メモリーの区域ｄ１１９ｄが有するインストラクション・コードにより、コンテンツプロバイダの識別子１２０に基づいて識別子の修正子を決定することができる。

区域ｅ１１９ｅが有するインストラクション・コードにより、暗号化を行うことができる。

できれば、それは対称暗号化であることが望ましい。

【００３１】

アクセスプロバイダのゲートウェイ１１２が有するメモリー１２１により、コンテンツプロバイダの識別子を、そのコンテンツプロバイダのコードと、作成すべき分離識別子の種類とに結びつけることができる。

【００３２】

図２は、本発明の分離識別子について考えられる構造である。図２が示す分離識別子２００には四つのフィールドが必要である。以下の説明では、「有する」という動詞を、フィールドを識別子に結びつけるために使う。しかしながら、それは必ずしもただ単に数値を並置するということではない。それらの数値もまた、アクセスプロバイダが行う可逆的方法に従って組み合わせることが可能である。

【００３３】

第一のフィールド２０１は、ネットワーク１１１上で通信機器１０１のユーザーを識別する識別子１１７に対応するものである。フィールド２０１により、アクセスプロバイダはユーザーを民事的に識別することが可能になる。例えば携帯電話のオペレーターの場合、フィールド２０１は携帯電話の番号の有効な数字を有するが、場合によっては、電話番号をユーザーに関連づけることを可能にするような契約の識別子２０５のこともある。契約番号を使用しないことは可能であるが、電話番号が別のユーザーに帰属している場合には、混乱を招く恐れがある。この契約番号は、電話番号を別のユーザーに新しく帰属させる場合に役に立つ。そのような契約番号は、例えば、電話通信番号の割当て数を数えるためのものである。第二のフィールド２０２は、ユーザーの要望や、コンテンツプロバイダのコードに応じて分離識別子２００を変化させる手段に対応している。フィールド２０２と２０１は組み合わされ、そして／または区域ｅ１１９ｅのインストラクション・コード

を用いてコード変換される。コード変換は、できれば、対称的暗号化であることが望ましい。コード変換は表に基づいて、あるいは一連の数に基づいて、ハッシュ関数に基づいて置換することによって行ってもよい。次に、暗号化の例を用いるが、可逆的なコード変換ならどんなタイプのものでもよい。その場合、分離識別子は、この組み合わせ－コード変換の結果であり、即ちアクセスプロバイダ以外の誰かには理解不能の一連のビットである。ここで理解不能というのは、民事的識別に関連づけるのが不可能という意味である。

【００３４】

一つの変形例として、分離識別子２００は、識別子を作成したアクセスプロバイダの識別を可能にするフィールド２０３や、例えば、分離識別子２００についてのバージョン及び／または種類のコード化を可能にするフィールド２０４を有する。

分離識別子２００は、アクセスプロバイダのゲートウェイ１１２とコンテンツプロバイダのサーバー１０２が通信する際の分離識別子１１８として用いられる。

コンテンツプロバイダのサーバー１０２のユーザー・メモリー１０６の列１０６ａの中に記録されているのは、分離識別子１１８である。

この変形例においては、その場合、分離識別子１１８は、フィールド２０３、２０４そして前の段落で述べた組み合わせ－コード変換の結果の並置である。

そういうわけで、コンテンツプロバイダによりコード変換されているために理解不能な部分が一部あり、コード変換されていないために理解可能な部分が一部ある。

【００３５】

図３は、本発明の方法を実施する手順を示している。

【００３６】

図３における、手順３０１においては、携帯電話である通信機器１０１が、コンテンツプロバイダのサーバー１０２に宛ててリクエストを送信している。

このリクエストが有するのは、ユーザーの識別子１１７、コンテンツプロバイダの識別子１２０および、リクエストそのものを有しているフィールド１２２である。

そのようなリクエストは、例えば、ＨＴＴＰプロトコルによって規定されるようなフォーマットでのＧＥＴリクエスト等である。

通信機器１０１が携帯電話であるので、この場合においては、プロトコルはＷＴＰが使われていることに注目すべきである。

手順３０１で作成され送信されたリクエストは、手順３０２でアクセスプロバイダのゲートウェイ１１２が受信する。

手順３０２でマイクロプロセッサー１１３は、リクエストからコンテンツプロバイダの識別子１２０を抽出する。

そして、該マイクロプロセッサー１１３は、このコンテンツプロバイダの識別子を探すため、メモリー１２１の表を検索する。

コンテンツプロバイダの識別子が見つかると、マイクロプロセッサー１１３は、このコンテンツプロバイダのコードと識別子の種類とを決定することができるようになる。

コンテンツプロバイダの識別子がメモリー１２１の表の中に見つからない場合には、マイクロプロセッサー１１３はデフォルトによる動作を適用する。

本例では、デフォルトによる動作は、セッションの分離識別子を作成することであると認められる。

【００３７】

一例としては、コンテンツプロバイダの識別子１２０は、ＩＰＶ４のフォーマットでのアドレスであることが望ましい。

それはまた、音声サーバーの電話番号であったり、ＳＭＳであったりしてもよい。

それはまた、ＩＰＶ６のフォーマットでのアドレスであってもよいし、あるいは、ＵＲＬやＥメールアドレスであってもよい。

【００３８】

コンテンツプロバイダの識別子１２０が、メモリー１２１の表の中でセッションの分離識別子の種類に対応する場合は、セッションの分離識別子を作成する手順３０３に移る。

そうでない場合は、コンテクストの分離識別子を作成する手順３０４に移る。

【００３９】

分離識別子の種類が、セッションの分離識別子であろうと、あるいは、コンテクストの分離識別子であろうと、どちらも構造は同一のものであり、それは、図２について説明されている構造である。

セッションの分離識別子とコンテクストの分離識別子との差は、第２フィールド２０２の内容である。

セッションの分離識別子の場合には、第２フィールド２０２は疑似乱数データを有する。

該疑似乱数データは、例えば１９７０年１月１日０時００分から経過した秒数等である。

該疑似乱数データは、例えばそのランダムエレメントが作成された時間によって起動された疑似乱数発生器が発生させた、どんな数であってもよい。

一般的には、疑似乱数データは、偶然に左右される数字である。

【００４０】

手順３０４において、第２フィールド２０２は、手順３０２でメモリー１２１に読み込まれるコンテンツプロバイダのコードに対応している。

【００４１】

フィールド２０４により、例えば、識別子の種類をコード化することが可能になる。

それゆえ、フィールド２０４は、識別子がセッションの分離識別子である場合には、ある一つの数値を有し、それがコンテクストの分離識別子である場合には、もう一つの別の数値を有する。

フィールド２０２の値が決定された時、マイクロプロセッサー１１３は、本発明による分離識別子を作成することができる。

マイクロプロセッサー１１３は、フィールド２０２とフィールド２０１から成るフィールドの集合を暗号化する。

つぎにマイクロプロセッサー１１３は、暗号化の結果をアクセスプロバイダのゲートウェイ１１２を管理するオペレーターの識別子のフィールド２０３と分離識別子の種類のフィールド２０４とに結びつける。

このようにして分離識別子１１８が得られる。

分離識別子のサイズはユーザーの識別子１１７のサイズと異なっていてもよいことを指摘しておく。

フィールド２０３と２０４はオプションとして選択可能であることも指摘しておく。

【００４２】

ひとたび分離識別子１１８が作成されると、コンテンツプロバイダのサーバー１０２に宛てたリクエストを作成して送信する手順３０５に移る。

手順３０５で作成されるリクエストは、分離識別子１１８と、コンテンツプロバイダの識別子のフィールド１２０とリクエストのフィールド１２３とを有している。

実際には、フィールド１２０と１２３は、フィールド１２０と１２２と同じである。

本例では、手順３０５で作成されるリクエストはＨＴＴＰフォーマットのものである。

その場合には、フィールド１２０は宛て先のＩＰアドレスである。

実際には、手順３０５でアクセスプロバイダのゲートウェイ１１２が作成するリクエストの（音声、ＳＭＳ、ＩＰ等の）フォーマットは、携帯電話である通信機器１０１のユーザーが接続しようとするサーバーと互換可能なものである。

【００４３】

分離識別子１１８のフィールドは、図２に関して説明したフォーマットでのフィールドである。

そういうわけで、分離識別子１１８が有するのは、分離識別子を作成したオペレーターを識別するフィールドと、それがセッションについてのものかそれともコンテクストについてのものかに応じて分離識別子の種類をコード化することのできるフィールドと、暗号

化されたフィールドである。
暗号化されたフィールドは、ひとたび暗号が解かれると、二つのフィールドを有する。
これら二つのフィールドは、第１フィールド２０１と第２フィールド２０２に対応している。
コンテンツプロバイダは暗号を解くことが不可能であり、したがって、フィールド２０１と２０２にアクセスすることが不可能である。
【００４４】
リクエストを送信した後、手順３０５で送信されたリクエストをコンテンツプロバイダのサーバー１０２で受信する手順３０６に移る。
それゆえ、手順３０６でコンテンツプロバイダのサーバー１０２は、分離識別子１１８と１２３のフィールドにアクセスすることができる。
分離識別子１１８によりコンテンツプロバイダのサーバー１０２は、ユーザー・メモリー１０６の表を参照してサーバー１０２に接続するユーザーについての一定数の情報を検索することができる。
実際には、セッションの分離識別子に関する場合にはユーザーについての情報をユーザー・メモリー１０６の表が有する公算は低い。
事実、セッションの分離識別子はセッション毎に変化するのであり、同一のユーザーが同じセッションの分離識別子でコンテンツプロバイダのサーバー１０２に二度接続することはない。
本説明に関しては、セッションとは、例えば１５分に限定された一時的な継続時間を意味する。
セッションの継続時間が簡単に測定可能なのは、本発明によるセッション分離識別子が、例えば、作成または期限の日付の情報を有しているからである。
【００４５】
コンテクストの分離識別子の有効期間は、もっとずっと長く、例えば六ヵ月から十八ヵ月、それどころか、もっと長くなることもある。
コンテクストの分離識別子の有効期間の管理は、例えば、暗号化するのに用いられるキーによって行うが、その暗号化はコンテクストの分離識別子の有効期間の頻度で変化するものである。
コンテクストの識別子の有効期間はまた、コンテクストの識別子の有効期間の頻度を変える第２フィールド２０２のコンテンツによって管理してもよい。
フィールド２０４を用いる変形例においては、コンテクスト分離識別子は、したがって、フィールド２０４によって種類づけされ、かつ、作成日付を含んでいる。
コンテクスト分離識別子は、その場合、例えば月または年で表された有効期間を含む。
【００４６】
有効期間とその管理の仕方とをどう選ぶかは、アクセスプロバイダのゲートウェイ１１２の責任を負うエンティティに帰するものである。
有効期間が保証されているという事実により、コンテンツプロバイダは、これもまたコンテクストと呼ばれる情報をその分離識別子に結びつけることができる。
【００４７】
手順３０６で取りうる行動のうちで、コンテンツプロバイダのサーバー１０２は、分離識別子１１８に基づいて、アクセスプロバイダのゲートウェイ１１２に向けてサービスのリクエストを作成し送信することができるが、それが手順３０７であって、ユーザー・メモリー１０６の表の中に情報を記録することができるのが手順３０８で、そして、携帯電話である通信機器１０１のユーザーのリクエストへの応答を作成し送信することができるのが手順３０９である。
【００４８】
手順３０５で送信されたリクエストへの応答をコンテンツプロバイダのサーバー１０２が作成する場合には、応答フォーマットが構成されるが、それは、ユーザーを識別する分離識別子１１８のフィールドと、その応答を実行するコンテンツプロバイダのサーバーの

識別子１２０を有するフィールドと、その場合のそのリクエストへの応答を有するフィールド１２３とを有するものである。
この応答は、アクセスプロバイダのゲートウェイ１１２に宛てられる。
手順３１０においては、アクセスプロバイダのゲートウェイ１１２は手順３０１で送信されたリクエストへの応答を受信する。
そこでアクセスプロバイダのゲートウェイ１１２は、分離識別子１１８とユーザーの識別子１１７との間のコード変換を行い、それにより、携帯電話である通信機器１０１にコンテンツプロバイダのサーバーからの応答を伝送する。
そこで手順３１１に移り、手順３０１で送信したリクエストへの応答を通信機器１０１によって受信する。

【００４９】
手順３１０では、識別子のコード変換と共に識別子の有効性の検証を行ってもよい。
この検証は、例えば、分離識別子１１８の暗号化された部分の暗号を解き、そうして第２フィールド２０２の値を回収した後に行われる。
その場合の有効化は、識別子の種類で決まる。
それがセッションの分離識別子である場合には、第２フィールド２０２はある日付に対応している。
そこで、その日付を、応答が受信された日付と比較する。
それら二つの日付の差が予め定められた期限、例えば１５分を越えている場合には、そのリクエストは無効とされ、通信機器１０１に再伝送されることはない。

【００５０】
それがコンテクストの分離識別子である場合には、第２フィールド２０２の内容を、メモリー１２１の表の中のコンテンツプロバイダの識別子１２０に対応する行について、コードのフィールドの内容と比較する。
一致すればそのリクエストは有効であり、そうでなければ、そのリクエストは拒絶される

【００５１】
手順３０７においては、コンテンツプロバイダのサーバー１０２がアクセスプロバイダのゲートウェイ１１２宛てのサービス・リクエストを送信する。
このリクエストは、ユーザーの分離識別子と、コンテンツプロバイダの識別子と、リクエストのフィールドとを有している。
そのようなリクエストは、例えば、ユーザーの識別依頼、ユーザーの所在地特定の依頼、加入者／ユーザーへのメッセージの送信依頼、あるいは、そのユーザーがコンテンツプロバイダのサーバー１０２に接続するために用いる機器の種類についての情報の依頼に関するものであってよい。これら列挙したものは、すべてを網羅しているわけではない。
アクセスプロバイダのゲートウェイ１１２は、手順３１２で、サービスを依頼するリクエストを受信する。
手順３１２では、アクセスプロバイダのゲートウェイ１１２はまずその分離識別子の有効性を検証する。
この検証は、前述の通りに行われる。
その識別子が有効でないなら、終わりの手順３１９に移り、アクセスプロバイダのゲートウェイ１１２は、そのサービス・リクエストを実行に移したりはしないが、そうでなければ、サービス・リクエストに応える手順３１４に移る。

【００５２】
本発明の変形例の一つにおいては、メモリー１２１の表は、さらに、各コンテンツプロバイダに関して、コンテンツプロバイダが要求しうるサービスのリストを有している。
手順３１３においては、アクセスプロバイダのゲートウェイ１１２は、その場合、リクエストを送信するコンテンツプロバイダが確かにそのリクエストを送信する権利があるのか、つまりそのサービスを要求する権利があるのかを検証する。
もしそうなら、アクセスプロバイダのゲートウェイ１１２は、そのサービス・リクエス

トへの応答を作成し、応答をコンテンツプロバイダのサーバー１０２に伝送する。
そうでなければ、そのサービス・リクエストへの応答はない。
【００５３】
手順３１４では、コンテンツプロバイダのサーバー１０２は、そのサービス・リクエストへの応答を受信する。
この応答により、コンテンツプロバイダのサーバー１０２は、ユーザー・メモリー１０６の表を更新したり、あるいは、手順３０９の応答を作成したりすることができる。
実際には、手順３０１で発信されたリクエストは、ユーザーのいる場所に近いレストランのリストを知りたいというリクエストであったというようなことが想定できる。
その場合には、コンテンツプロバイダのサーバー１０２は、そのユーザーの位置を知る必要があり、それゆえ、コンテンツプロバイダのサーバー１０２は、アクセスプロバイダのゲートウェイ１１２に向けて、位置特定依頼を発信することになる。
位置特定の応答により、コンテンツプロバイダのサーバー１０２は、通信機器１０１のユーザーに相応しい応答を送ることができる。
【００５４】
本発明による識別子により、コンテンツプロバイダのサーバー１０２は、手順３１５で、新しく入ってくるリクエストを通信機器１０１宛てに送信することもできる。
この新しく入ってくるリクエストを、その時、手順３１６で受信するのがアクセスプロバイダのゲートウェイ１１２である。
この新しく入ってくるリクエストを、分離識別子１１８の検証作業に掛ける。
この検証作業は、手順３１０と３１２と３１３に関して説明した検証と同じものである。
つまり、フィールド１２０によって識別されたコンテンツプロバイダは新しく入ってくるリクエストを送信する資格がなければならず、更に、分離識別子１１８が有効でなければならない。
識別子が有効でない場合には、終わりの手順３１９に移るが、そこではコンテンツプロバイダのサーバー１０２が送信した新しく入ってきたリクエストには一切、応えない。
【００５５】
手順３１５で送信された新しく入ってきたリクエストが有効であることが手順３１６で明らかになった場合には、アクセスプロバイダのゲートウェイ１１２が分離識別子１１８をユーザーの識別子１１７に向けてコード変換し、コード変換された新しく入ってきたリクエストを携帯電話である通信機器１０１に伝送する。
手順３１７では、携帯電話である通信機器１０１が、その新しく入ってきたリクエストを受信して処理する。
そのような新しく入ってきたリクエストは、例えば、通信機器１０１の中のデータベースの更新であったりする。
そのようなデータベースは、例えば、通信機器１０１のユーザーが維持したいと願っている連絡先に関するものであってもよいし、あるいは、通信機器１０１が接続して様々なサービスにアクセスすることができるサーバーのリストに関するものであってもよい。
【００５６】
第１フィールド２０１と第２フィールド２０２を暗号化するために用いられる暗号化アルゴリズムは、できれば、ＤＥＳまたは３ＤＥＳであることが望ましい。
それは、ブロック暗号化バージョンでも、あるいは、ブロック連鎖による暗号化バージョンのものでもよい。
ブロック連鎖による暗号化を行うバージョンにより、分離識別子２００の暗号化された部分のすべては、可変性の第２フィールド２０２のおかげで、確実に異なったものにすることができる。
本発明の幾つかの変形例においては、例えばＡＥＳ（Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）のような他の暗号化アルゴリズムを用いてもよい。
【００５７】

本発明および、本発明によって規定されるコンテクストの分離識別子の利点の一つは、ユーザー用に、コンテンツプロバイダごとに異なるコンテクスト識別子を持てるということである。

従って、あるコンテンツプロバイダが、識別子で識別されたあるユーザーの私生活の情報がもっとよく分かるように、他のコンテンツプロバイダのデータベースと、自分のデータベースとを突き合わせてチェックするということはできないようになっている。

コンテンツプロバイダは、ユーザーの民事的身元についても、同一のユーザーが常に同一の分離識別子で接続するかどうかについても、何の確証も持っていないのだから、コンテンツプロバイダがアクセスプロバイダのデータベースを盗用することも不可能である。

そういうわけで、そのようにして、ユーザーのプライバシーは最大限の保護が得られることになる。

【００５８】

一つの識別子に基づいて、識別子を作成したオペレーターだけが、アクセスプロバイダの協力を得て、物理的なユーザーまで逆上っていくことが可能なのだから、法的な要請も満足させることができる。

【００５９】

あるユーザーが、常にセッション識別子を使用して接続することを選ぶのも可能である。

この場合、時間的に適度な間を置いた二つの接続については、そのような選択を行ったユーザーは二つの異なる分離識別子を提示して同一のサイトに接続することになる。

その場合、コンテンツプロバイダには、それが同一のユーザーで接続を二回行ったのだということをつきとめる手段は全くないことになる。

【００６０】

あるユーザーが、コンテクスト識別子を用いるということを選択することも可能である。

その場合は、アクセスプロバイダのゲートウェイ１１２が、その選択を行ったユーザーの接続に際して、コンテクストの分離識別子を作成することになる。

その場合、コンテンツプロバイダは、コンテクストの分離識別子に関連づけることのできる情報に応じて、その応答を適応させることができることになる。

【００６１】

このユーザーの選択は、アクセスプロバイダのゲートウェイ１１２において、識別子１１７のようなユーザーの識別子を、ユーザーの選択に結びつける表を介して管理される。

【００６２】

本発明は、インターネットアクセスプロバイダ（略してＩＳＰ）を介してコンテンツプロバイダへと、パソコンを使って接続するユーザーを想定する場合にも、完全に転換可能である。

その場合には、パソコンをゲートウェイに接続するモードは（ＧＳＭ，ＵＭＴＳ等の）電波によるもの、（交換電話ネットワーク等の）有線のもの、あるいはその他のものがある。

【００６３】

そういうわけで、本発明には、分離識別子を管理するエンティティが、そのような分離識別子を蓄積しなくともよいようにできるという利点がある。

事実、そのような識別子の計算は、その計算の時点で簡単にアクセスできるデータに基づいて行われるので、それらを蓄積する必要はない。

【００６４】

結局のところ、本発明の分離識別子は、インターネットのネットワーク上で用いられる何らかのプロトコルのフレームにおけるのと同様に、電話通信の規準のＮＤＳフィールドにおいても搬送されていく。それゆえ、本発明の分離識別子は普遍的であり、それにより、中でも、同一のコンテンツプロバイダの様々に異なるタイプのサーバーに、同一のコンテクスト分離識別子を用いてユーザーが接続することができるようになる。それにより、

コンテンツプロバイダのタスクが大いに単純化され、コンテンツプロバイダはサーバーのタイプに関わらずコンテクストの管理を統一して行うことができる。

【図面の簡単な説明】

【００６５】

【図１】本発明の方法を実施するために有用な手段を示す概略図

【図２】本発明の分離識別子の構造の概略図

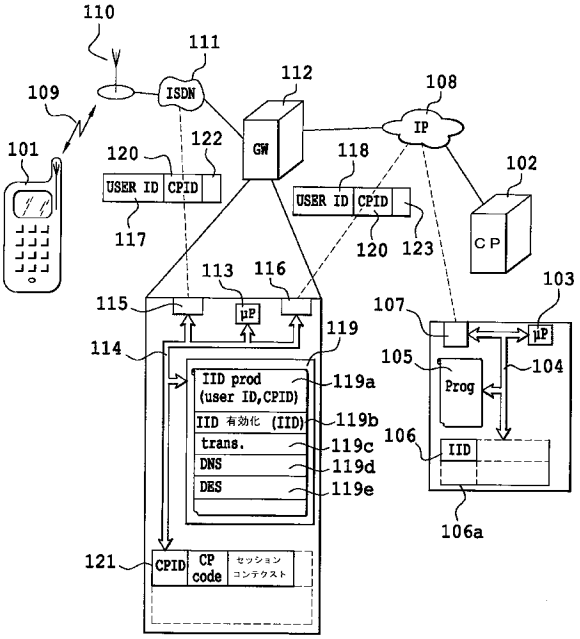
【図３】本発明の方法を実施する手順の概略図

【符号の説明】

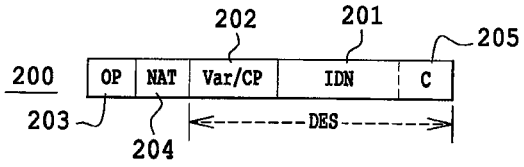
【００６６】

１０１　通信機器
１０２　コンテンツプロバイダのサーバー
１０３　マイクロプロセッサー
１０４　バス
１０５　プログラム・メモリー
１０６　ユーザー・メモリー
１０７　インターフェイス回路
１０８　インターネット
１０９　無線接続
１１０　基地局
１１１　ＩＳＤＮネットワーク
１１２　アクセスプロバイダのゲートウェイ
１１３　マイクロプロセッサー
１１４　バス
１１５　インターフェイス回路
１１６　インターフェイス回路
１１７　ユーザーの識別子
１１８　分離識別子
１１９　プログラム・メモリー
１１９ａ　区域ａ
１１９ｂ　区域ｂ
１１９ｃ　区域ｃ
１１９ｄ　区域ｄ
１１９ｅ　区域ｅ
１２０　コンテンツプロバイダの識別子
１２１　メモリー
２００　分離識別子

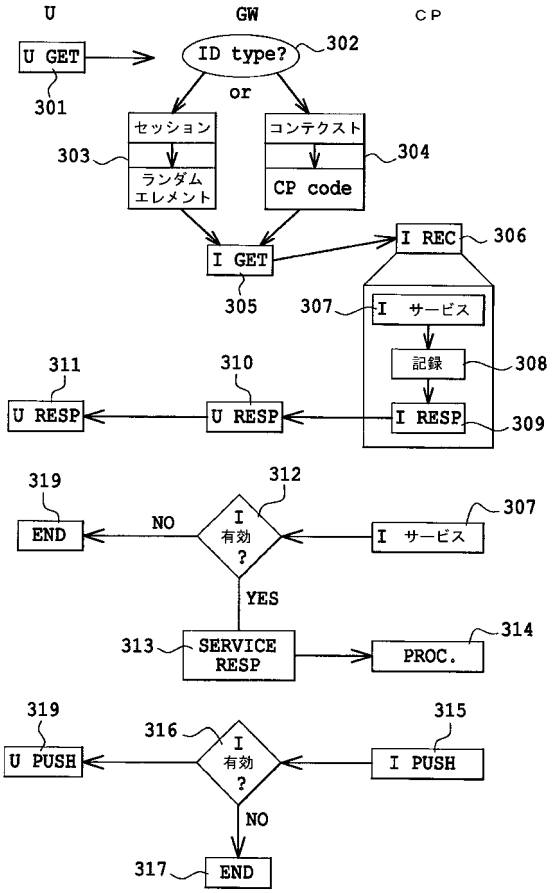
【図１】


110
111
112
108
109
ISDN
GW
IP
101
120
122
118
102
USER ID
CPID
USER ID
CPID
CP
117
120
123
113
116
103
115
μP
μP
107
119
114
105
Prog
104
IID prod
(user ID,CPID)
119a
IID 有効化 (IID)
119b
trans.
119c
106
IID
DNS
119d
DES
119e
106a
121
CPID
CP code
セッション
コンテクスト

【図２】


202
201
205
200
OP
NAT
Var/CP
IDN
C
203
204
DES

【図３】


U
GW
CP
U GET
ID type?
302
301
or
セッション
コンテクスト
303
304
ランダム
エレメント
CP code
I GET
I REC
306
305
307
I サービス
記録
308
311
310
U RESP
U RESP
I RESP
309
319
312
END
NO
I
有効
?
I サービス
307
YES
313
SERVICE
RESP
PROC.
314
319
316
315
U PUSH
I
有効
?
I PUSH
NO
317
END

フロントページの続き

【要約の続き】
【選択図】図１