(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2014-182828
(P2014-182828A)
(43)公開日　平成26年9月29日(2014.9.29)

(51)Int.Cl.		F I		テーマコード（参考）
G06F 13/00	(2006.01)	G06F 13/00	540E	5B084

審査請求 未請求　請求項の数 20　ＯＬ　外国語出願　（全 13 頁）

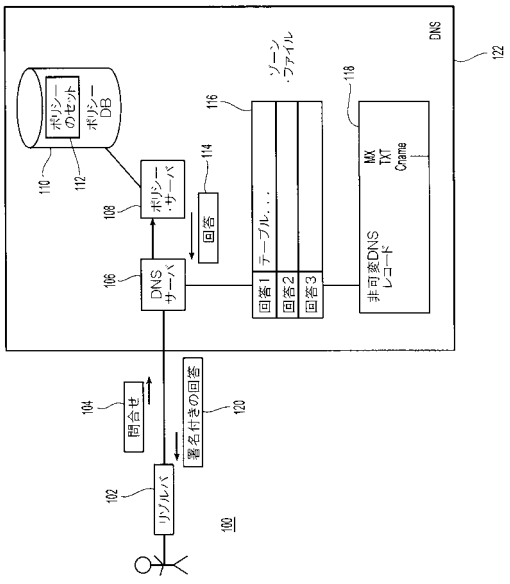
(21)出願番号　特願2014-51475(P2014-51475)
(22)出願日　平成26年3月14日(2014.3.14)
(31)優先権主張番号　61/800,405
(32)優先日　平成25年3月15日(2013.3.15)
(33)優先権主張国　米国(US)
(31)優先権主張番号　14/092,528
(32)優先日　平成25年11月27日(2013.11.27)
(33)優先権主張国　米国(US)

(71)出願人　502377350
ベリサイン・インコーポレイテッド
アメリカ合衆国・ヴァージニア・２０１９０・レストン・ブルーモント・ウェイ・１２０６１
(74)代理人　100112737
弁理士　藤田　考晴
(74)代理人　100118913
弁理士　上田　邦生
(74)代理人　100136168
弁理士　川上　美紀

最終頁に続く

(54)【発明の名称】レコード・セットへのＤＮＳＳＥＣ対応ゾーンの事前署名のためのシステムおよび方法

(57)【要約】　（修正有）
【課題】レコード・セットへのＤＮＳＳＥＣ対応ゾーンの事前署名を行うためのシステムおよび方法を提供する。
【解決手段】ドメイン・ネーム・システム１２２は、Ｗｅｂドメインのための、セキュリティ拡張方式のドメイン・ネーム解決（ＤＮＳＳＥＣ）を制御するために、管理者、またはＤＮＳ運用者自体が希望するＤＮＳポリシーのセットを受信し、受信したポリシーのセットに基づいて、ドメインに向けられたユーザの問合せに対する回答のセットを生成することができる。ポリシー規則に基づいて異なる、または変動するこれらの回答は、可変回答として格納することができ、また可変ＩＤでラベル付け可能である。可変回答は、事前署名し、ＤＮＳに格納することができる。ＤＮＳ要求が受信される前に、鍵データおよび他の情報が生成され、格納されているので、要求された可変回答を、より優れた応答性およびセキュリティで返すことができる。
【選択図】図１



【特許請求の範囲】
【請求項１】
ドメイン・ネーム・システム運用を行う方法であって、
ドメイン・ネーム・システム・セキュリティ拡張（ＤＮＳＳＥＣ）を使用して、ドメイン・ネーム・システム（ＤＮＳ）の運用のためのポリシーのセットにアクセスするステップと、
前記ポリシーのセットに基づいて、ゾーンのドメイン・ネームのセットに関連する問合せに対する回答のセットを生成するステップと、
前記回答のセットおよび鍵データのセットから、署名付きの回答のセットを生成するステップと、
前記署名付きの回答のセットをゾーン・ファイルに格納するステップと、
リゾルバから、問合せを受信するステップと、
前記リゾルバに送信するために、前記リゾルバから受信した前記問合せおよび前記ポリシーのセットに基づいて、署名付きの回答を検索するステップと
を含む方法。
【請求項２】
前記ポリシーのセットにアクセスするステップが、前記ドメイン・ネームのセットに関連するユーザからポリシーのセットを受信するステップを含む請求項１に記載の方法。
【請求項３】
前記ポリシーのセットにアクセスするステップが、前記ＤＮＳによって生成されるポリシーを適用するステップを含む請求項１に記載の方法。
【請求項４】
前記ポリシーのセットにアクセスするステップが、デフォルト・ポリシーのセットを設定するステップを含む請求項１に記載の方法。
【請求項５】
署名付きの回答のセットを生成するステップが、前記鍵データに格納された公開鍵と秘密鍵とのセットを使用して、前記署名付きの回答のセットを生成するステップを含む請求項１に記載の方法。
【請求項６】
前記ポリシーのセットが、
地理位置情報データに基づくポリシー、
負荷分散データに基づくポリシー、
時刻情報に基づくポリシー、
許可レベルに基づくポリシー、または
トラフィック管理規則に基づくポリシー
のうちの少なくとも１つを含む請求項１に記載の方法。
【請求項７】
回答のセットを生成するステップが、前記リゾルバおよび前記ポリシーのセットに関連するインターネットプロトコル（ＩＰ）アドレスに基づいて、回答のセットを生成するステップを含む請求項１に記載の方法。
【請求項８】
前記回答のセットが、
前記ドメイン・ネームのセットに関連する、インターネットプロトコル（ＩＰ）データのセット、
前記ドメイン・ネームのセットに関連する所有権情報、
前記ドメイン・ネームのセットに関連するクラス情報、
前記ドメイン・ネームのセットに関連する開始情報、または
前記ドメイン・ネームのセットに関連する有効期限情報
のうちの少なくとも１つを含む請求項１に記載の方法。
【請求項９】

前記ポリシーのセットを更新するステップをさらに含む請求項１に記載の方法。
【請求項１０】
前記更新されたポリシーのセットに基づいて、前記回答のセットを更新するステップをさらに含む請求項９に記載の方法。
【請求項１１】
ゾーン向けのドメイン・ネームのセットに関連する問合せを送信するリゾルバとのネットワーク・インターフェースであって、前記ドメイン・ネームが、ドメイン・システム・セキュリティ拡張（ＤＮＳＳＥＣ）下で動作する、ネットワーク・インターフェースと、
前記ネットワーク・インターフェースを介して前記リゾルバと通信するプロセッサであって、
前記ドメイン・ネーム・システム（ＤＮＳ）の運用のためのポリシーのセットにアクセスするステップと、
前記ポリシーのセットに基づいて、ドメイン・ネームのゾーンのセットに関連する問合せに対する回答のセットを生成するステップと、
前記回答のセットおよび鍵データのセットから、署名付きの回答のセットを生成するステップと、
前記署名付きの回答のセットをゾーン・ファイルに格納するステップと、
前記リゾルバから、前記問合せを受信するステップと、
前記リゾルバに送信するために、前記問合せおよび前記ポリシーのセットに基づいて、署名付きの回答を検索するステップと
を行うように構成されたプロセッサと
を備えるシステム。
【請求項１２】
前記ポリシーのセットにアクセスするステップが、前記ドメイン・ネームに関連するユーザから、ポリシーのセットを受信するステップを含む請求項１１に記載のシステム。
【請求項１３】
前記ポリシーのセットにアクセスするステップが、前記ＤＮＳによって生成されるポリシーを適用するステップを含む請求項１１に記載のシステム。
【請求項１４】
前記ポリシーのセットにアクセスするステップが、デフォルト・ポリシーのセットを設定するステップを含む請求項１１に記載のシステム。
【請求項１５】
署名付きの回答のセットを生成するステップが、前記鍵データに格納された公開鍵と秘密鍵とのセットを使用して、前記署名付きの回答のセットを生成するステップを含む請求項１１に記載のシステム。
【請求項１６】
前記ポリシーのセットが、
地理位置情報データに基づくポリシー、
負荷分散データに基づくポリシー、
時刻情報に基づくポリシー、
許可レベルに基づくポリシー、または
トラフィック管理規則に基づくポリシー
のうちの少なくとも１つを含む請求項１１に記載のシステム。
【請求項１７】
回答のセットを生成するステップが、前記リゾルバおよび前記ポリシーのセットに関連するインターネットプロトコル（ＩＰ）アドレスに基づいて、回答のセットを生成するステップを含む請求項１１に記載のシステム。
【請求項１８】
前記回答のセットが、
前記ドメイン・ネームのセットに関連する、インターネットプロトコル（ＩＰ）データ

のセット、
前記ドメイン・ネームのセットに関連する所有権情報、
前記ドメイン・ネームのセットに関連するクラス情報、
前記ドメイン・ネームのセットに関連する開始情報、または
前記ドメイン・ネームのセットに関連する有効期限情報
のうちの少なくとも１つを含む請求項１１に記載のシステム。
【請求項１９】
前記プロセッサがさらに、前記ポリシーのセットを更新するように構成された請求項１１に記載のシステム。
【請求項２０】
前記プロセッサがさらに、前記更新されたポリシーのセットに基づいて、前記回答のセットを更新するように構成された請求項１９に記載のシステム。

【発明の詳細な説明】
【技術分野】
【０００１】
（関連出願の相互参照）
その内容が参照により本明細書に明白に組み込まれている、２０１３年３月１５日に出願した米国特許仮出願第６１／８００，４０５号、名称「Ｓｙｓｔｅｍｓ ａｎｄ Ｍｅｔｈｏｄｓ ｆｏｒ Ｐｒｅ－Ｓｉｇｎｉｎｇ ｏｆ ＤＮＳＳＥＣ Ｅｎａｂｌｅｄ Ｚｏｎｅｓ ｉｎｔｏ Ｒｅｃｏｒｄ Ｓｅｔｓ」の優先権が主張されている。
【０００２】
本教示は、レコード・セットへのＤＮＳＳＥＣ対応ゾーンの事前署名を行うためのシステムおよび方法に関し、より詳細には、ＤＮＳシステム・ポリシーに基づく、事前署名付きの鍵署名データを用いた、ドメイン・ネーム・システムからの、回答の生成を管理するプラットフォームおよび技法に関する。
【背景技術】
【０００３】
Ｗｅｂサイトおよび他のリソースの、インターネットおよび他のネットワーク上での位置の特定に使用されるドメイン・ネーム・システム（ＤＮＳ）の進化の過程で、時が経つにつれてセキュリティの問題が重要性を増している。進化するセキュリティ・ニーズに応え、業界内の組織は、ＤＮＳサービスの配信にセキュリティ対策の導入を可能にできるよう、基準線となるＤＮＳプロトコルに対し、拡張の提案および開発を行ってきた。一般に、これらの既知の標準は、ＤＮＳセキュリティ拡張、またはＤＮＳＳＥＣと呼ばれる。
【発明の概要】
【０００４】
具体的には、Ｗｅｂブラウザまたは他のソフトウェアを実行するユーザが、既知のＵｎｉｖｅｒｓａｌ Ｒｅｓｏｕｒｃｅ Ｌｏｃａｔｏｒ（ＵＲＬ）に移動しようとする際に自身に配信されるインターネットプロトコル（ＩＰ）アドレスが本物であり、ユーザがアクセスしようとしているＷｅｂサイトを表すことが保証されるようにする必要が生じている。所与のドメイン・ネームのＩＰアドレス、もしくはＤＮＳシステムによって提供される他の回答を検索し、提供するために使用されるＤＮＳサーバに対するキャッシュポイズニングまたは他の攻撃が原因で、偽のＩＰアドレスが、無意識のユーザに配信されるおそれがある。
【０００５】
Ｗｅｂサイトの展開に関して、多くのＷｅｂサイトは、今日、いくつかの階層区分または階層区画からなり、そのそれぞれは異なる拡張ドメイン・ネームを有している。例えば、スポーツ・ニュースに関係するＷｅｂサイトは、ＳｐｏｒｔｓＰａｇｅ．ｃｏｍなどのルート・レベルのほか、個々のスポーツ活動に専用のいくつかの区分または「ゾーン」を有する場合がある。こうしたトピックは、例えば、Ｇｏｌｆ．ＳｐｏｒｔｓＰａｇｅ．ｃ

ｏｍ、およびＳｏｃｃｅｒ．ＳｐｏｒｔｓＰａｇｅ．ｃｏｍなどのドメインに反映されることもあり得る。

【０００６】

ＳｐｏｒｔｓＰａｇｅ．ｃｏｍ内を移動中のユーザは、ＩＰアドレスまたは他の情報などを求める、１つもしくは複数の問合せまたは要求を、そのＷｅｂサイトをサポートするＤＮＳシステムに行うことができる。ユーザの問合せに対する回答は、そのＷｅｂサイトの様々なゾーン内から生成されてもよい。ユーザが確実に有効な回答を受信するために、ＤＮＳＳＥＣ対応ドメインは、一連のメッセージが、公開鍵／秘密鍵情報を使用して生成された署名を用いて署名済みであることを要求する。したがってＤＮＳＳＥＣプロトコルが、Ｗｅｂプロパティを検索しているユーザに認証サービスを提供している間、ドメインのゾーンにおける深さおよび階層のリンクがより複雑になり、そのため、ＤＮＳシステムの処理リソースおよび帯域幅リソースへの負荷が拡大する。その負荷は、ＤＮＳの応答性を低下させるおそれがある。

【０００７】

さらに、ＤＮＳＳＥＣ構成を使用しながら柔軟なＤＮＳポリシーの適用を望むＷｅｂサイト所有者にとっては、問題はさらに複雑になりかねない。すなわち、いくつかのゾーンを備えた比較的リッチなＷｅｂサイトを展開する運用者は、そのＤＮＳ検索または回答が、ユーザのロケーション、時刻、サーバ負荷に基づいて、および／または他の要因に基づいて、ドメインの様々なサーバおよび／またはゾーンを対象にするよう、個々の要求元に対する、規則の適用を望む可能性がある。ユーザに関する情報の識別、適切なポリシーの適用、および続く、特定の回答が認証されるのを可能にする必要な署名の生成によって、同様に、パフォーマンスのほか、システムの応答性に対するユーザの認識に関して不利益が発生するおそれがある。

【課題を解決するための手段】

【０００８】

レコード・セットへのＤＮＳＳＥＣ対応ゾーンの事前署名を行うための方法およびシステムを提供することが望ましいことがあり得、そこでは、ドメイン・ネーム・システムは、ドメイン所有者から、任意のポリシーのセットを受け入れ、それらのポリシーを、事前生成された署名付きの回答のセットまたは他のゾーン・ファイルに変換し、またオンデマンドでの生成および／または署名を要する回答に基づくのではなく、格納されたリソース・レコードに基づいて、署名付きの回答をユーザに送信することができる。

【０００９】

本明細書に組み込まれ、本明細書の一部を構成する添付図面は、本教示の実装形態を示し、またその説明と共に、本教示の原則を説明する働きをする。

【図面の簡単な説明】

【００１０】

【図１】様々な実装形態による、レコード・セットへのＤＮＳＳＥＣ対応ゾーンの事前署名を行うためのシステムおよび方法において使用可能な全体的なドメイン・ネーム環境を示す図である。

【図２】様々な実装形態による、レコード・セットへのＤＮＳＳＥＣ対応ゾーンの事前署名を行うためのシステムおよび方法において使用可能なゾーン・ファイルのデータ構造を示す図である。

【図３】各実装形態による、レコード・セットへのＤＮＳＳＥＣ対応ゾーンの事前署名を行うためのシステムおよび方法で使用可能なポリシー検証、署名付きデータの生成、ならびに他の処理の流れ図である。

【図４】様々な実装形態による、レコード・セットへのＤＮＳＳＥＣ対応ゾーンの事前署名において使用可能な例示的なハードウェア、ソフトウェア、および他のリソースを示す図である。

【発明を実施するための形態】

【００１１】

本教示の実装形態は、レコード・セットへのＤＮＳＳＥＣ対応ゾーンの事前署名を行うためのシステムおよび方法に関する。より詳細には、実装形態は、ＤＮＳＳＥＣセキュリティを使用するＤＮＳ実装形態を管理するプラットフォームおよび技術に関する。そうした環境では、本教示によるプラットフォームおよび技術は、ＤＮＳ運用のための任意のポリシーのセットを受信することができ、そのポリシーによって、ドメイン・ネームを有効なＩＰアドレスまたはその他のものに解決するなどの、問合せに対する回答を求める要求を実行することができる。

【００１２】

ＤＮＳシステムは、ドメイン・ネーム所有者または運用者から、ポリシーのセットを受信し、それらのポリシーを、ＤＮＳシステム自体の内部の運用ポリシーに照らして検証し、また有効な回答を生成するために使用可能なポリシーを組み込むことができる。ポリシーのセットはまた、あるいは代わりとして、例えば、負荷分散または他の論理をＤＮＳインフラストラクチャに適用できるよう、ＤＮＳシステム自体の運用者によって供給された規則またはポリシーを含むことができる。ポリシー変数に基づいて変動する、または異なる回答を生成し、可変識別子によって索引付けされたゾーン・ファイルのリソース・レコード・セットに格納することができる。可変回答は、公開鍵／秘密鍵ペアで事前署名することができ、それにより、新しい問合せがＤＮＳシステムに到達したときに、ゾーン・ファイル・テーブルまたは他のレコードから、既に署名された有効な回答を検索し、要求元に送信することができる。

【００１３】

その結果、新しいドメイン・ネーム解決要求は、署名付きデータがオンザフライで生成されないので、より効率的に解決可能である。これらの運用はまた、公開鍵／秘密鍵データを、ＤＮＳプラットフォームをサポートしている様々なサーバに分散させる必要がないので、より安全に実行することができる。他の利点および利益も実現することができる。

【００１４】

以下、本教示の例示的な実装形態について詳述するが、それらは添付図面で示されている。可能であれば同一の参照番号は、複数の図を通じて、同一のまたは同様の部分を参照するために使用される。

【００１５】

図１は、諸態様による、レコード・セットへのＤＮＳＳＥＣ対応ゾーンの事前署名を行うためのシステムおよび方法が動作し得る全体的なＤＮＳ環境１００を示す。図に示すような態様では、ＤＮＳ環境は、ドメイン・ネーム・システム（ＤＮＳ）１２２と通信することで、問合せ１０４を通知し、署名付きの回答１２０を受信するリゾルバ１０２を含むことができる。本明細書で使用する署名付きの回答１２０は、署名付きのＤＮＳレコードを含む回答ということができる。ＤＮＳ１２２は、サーバ、分散サーバのセット、クラスタ、クラウドベース・サービス、アプライアンス、および／または他のハードウェア、リソース、プラットフォーム、もしくは要素である、もしくはそれらを含むことができる。

【００１６】

問合せ１０４は、例えば、所与のドメイン・ネームに関係するインターネットプロトコル（ＩＰ）アドレスを求める要求などの、ゾーン、および／または他のサイトもしくはロケーションへの様々な照会のいずれかであってもよいし、あるいはいずれかを含むことができる。ＩＰアドレスは、ＩＰｖ４（３２ビット）、ＩＰｖ６（１２８ビット）、および／または他の形式であることができる。問合せ１０４はまた、あるいは代わりとして、ロケーション情報、証明書情報、権限情報、サーバ情報、ネットワーク情報、および／または他の結果もしくは情報などの、ＤＮＳ１２２からの他の情報を求める要求であってもよい。リゾルバ１０２は、インターネット、および／または他のパブリック／プライベート・ネットワークもしくはチャネルを介して、ＤＮＳ１２２と通信することができる。リゾルバ１０２は、例えば、ドメイン・ネームの所有者もしくは運用者、これらのエンティティのシステム管理者、または他の人を含む幾人かの当事者が操作することができる。

【００１７】

ＤＮＳ１２２は、問合せ１０４を受信し、Ｉｎｔｅｒｎｅｔ Ｅｎｇｉｎｅｅｒｉｎｇ Ｔａｓｋ Ｆｏｒｃｅ（ＩＥＴＦ）および／または他の関連する標準化団体によって規定されているような、ＤＮＳセキュリティ拡張（ＤＮＳＳＥＣ）の標準と一致する署名付きの回答１２０を生成するように構成することができる。概して、ＤＮＳＳＥＣの利用には、ＤＮＳネットワークにおいて、所与のドメイン、そのドメインに関連するゾーン、および／もしくは他の要素をサポートするサーバ間の署名付きのメッセージまたはデータの交換の利用が含まれる。ＤＮＳクエリに回答を提供するサーバは、提供している情報を認証するために信頼の連鎖において次のサーバに送信する秘密鍵を使用して、その回答に署名を行うことができる。署名付きの回答または他のデータの受信者は、送信元サーバの公開鍵を使用して、データの信憑性を確認することができる。

【００１８】

図に示すようなＤＮＳ１２２は、様々なエンティティに対し、ＤＮＳプラットフォームまたはサービスをホスティング提供または管理することができる。例えば、ＤＮＳ１２２は、自身のＤＮＳ運用が外部の供給元によって提供されることを望んでいる第三者の加入者にＤＮＳサービスを提供することができる。ＤＮＳ１２２は、同様に、エンティティ自身のネットワークに対するＤＮＳサービスをサポートするために利用可能であり、また他の構成下のＤＮＳサービスをサポートすることができる。

【００１９】

ＤＮＳ１２２は、概して、ＤＮＳＳＥＣ対応のＤＮＳ運用を実行するためのいくつかの要素またはリソースを組み込むことができるほか、受信した問合せまたは要求に対する回答を決定するためのポリシーのセット１１２を使用することができ、その受信した問合せまたは要求は、ドメイン・ネーム、および／もしくはそのドメイン・ネームに関連するゾーンのセットに関係する、または関連付けられている可能性がある。ＤＮＳ１２２は、ポリシー・サーバ１０８と通信して、問合せ１０４に対する回答１１４を生成する、または検索するＤＮＳサーバ１０６（複数可）を組み込むことができる。回答１１４は、前述のように、ポリシーのセット１１２に基づいて、生成する、または検索することができ、ポリシーのセット１１２は、ポリシー・データベース１１０に格納する、かつ／またはＤＮＳ１２２内にホスティング提供された、もしくはＤＮＳ１２２と関連付けられた他のデータストアに格納することができる。各態様によれば、ポリシーのセット１１２を、問合せ１０４および／または回答１１４に適用して、問合せ１０４に応答する、事前生成された情報セットを作成することができる。この事前生成された情報は、ポリシーのセット１１２に規定された、変数およびポリシーによって異なる、または変動する情報、ならびにポリシーのセット１１２に規定された、変数およびポリシーによって異なることのない、または変動することのない情報に区分することができる。

【００２０】

ポリシーのセット１１２は、リゾルバの問合せ１０４に対する回答１１４が生成され、要求ユーザに供給される根拠となる条件を決定するスクリプトのセット、または他の論理、プログラミング、条件、もしくは規則である、あるいはそのいずれかを含むことができる。ポリシーのセット１１２は、例えば、特定の地理的領域を用いて要求を行うユーザのＩＰアドレスは、ＤＮＳ１２２と関連付けられた特定のサーバに向けることができると規定した地理位置情報規則を含むことができる。問合せ１０４が受信される時点などの時刻に基づく規則も適用することができる。ポリシーのセット１１２はさらに、ＤＮＳ１２２と関連付けられたサーバへの負荷のバランスを取るために、負荷分散基準に基づく規則を含むことができる。ポリシーのセット１１２は、同様に、他の規則、テスト、発見的方法、またはポリシーを含むことができる。例えば、ポリシーのセット１１２は、参照によりその全体が本明細書に組み込まれている、Ｄａｎｉｅｌ ＪａｍｅｓおよびＡｒｕｎａｂｈｏ Ｄａｓの２０１３年３月１５日に出願した同時係属中の特許文献１、名称「Ｈｉｇｈ Ｐｅｒｆｏｒｍａｎｃｅ ＤＮＳ Ｔｒａｆｆｉｃ Ｍａｎａｇｅｍｅｎｔ」、代理人整理番号１１５６９．０２１０で説明され、かつこの出願と同じエンティティに割り当てられる、もしくは割り当てられなければならないといった規則または論理を含むことが

できる。

【００２１】

ポリシーのセット１１２は、事例では、ＤＮＳ１２２によってサポートされたドメイン・ネームの所有者または運用者によって供給可能である。ポリシーのセット１１２はまた、あるいは代わりとして、ＤＮＳ１２２自体の所有者または運用者によって、かつ／または他のユーザもしくは供給元によって規定されてもよい。

【００２２】

ＤＮＳ１２２は、ポリシーのセット１１２の受信および設定の後、各実装形態において、リゾルバ１０２および／または他のユーザによって提供されたポリシーがＤＮＳ１２２の内部運用と決して衝突しないように、それらのポリシーを、ＤＮＳ１２２の内部の規則もしくはポリシーに照らして確認する、または検証することができる。別の各実装形態によれば、リゾルバ１０２および／または他のユーザが、必要なポリシーのフルセットの供給に失敗した場合、ＤＮＳ１２２は、デフォルトの規則またはポリシーを、関連するドメイン・ネームの運用に適用することができる。

【００２３】

ポリシーのセット１１２が設定された後、ＤＮＳ１２２は、その規則または論理のセットを使用して、ドメイン・ネームおよび／またはその関連ゾーンに関係する回答を生成することができる。各態様によれば、図１に示すように、回答は、ゾーン・ファイル１１６内で符号化することができる。ゾーン・ファイル１１６は、ポリシーのセット１１２に基づく考え得るそれぞれの回答に対し、識別子（例えば、図に示すような回答１、回答２、回答３など）によって索引付けされたテーブルの形で格納することができる。各実装形態では、あるドメイン向けのポリシーのセット１１２および関連するドメイン・ネーム・レコードを前提として、問合せ１０４に対する考え得るすべての回答を生成する、または理解することが可能となり得る。事例では、例えば、回答の総数は、５、１０、または考え得る回答の別の数など、比較的少ない場合がある。少数の回答は、システムの応答性の向上に貢献し得るが、回答のより多数の集合が、生成され、格納される場合も同様にあることが理解されよう。

【００２４】

ＤＮＳ１２２によって作成された回答は、図に示すように、２つの包括的なグループに区分することができる。ポリシーのセット１１２および／または他の要因に基づいて異なる、または変動するグループと、そうではないグループである。変動する回答は、前述のように、こうした動的に選択された回答の１つを必要とする問合せ１０４が受信されたときの検索のために、ゾーン・ファイル１１６に「可変回答」として格納可能である。これらの可変回答は、可変ＩＤに基づいて索引付けまたはキー付けすることができ、また対応する問合せ１０４が受信されたときに、検索し、リゾルバ１０２に送ることができる。可変回答データは、例えば、様々なサービス・ロケーション向けの様々なＩＰアドレス値を含むことができ、かつ／または様々な別名（ＣＮＡＭＥ）および他の情報を含むことができる。変動しない回答は、非可変ＤＮＳレコード１１８に格納可能である。例えば、非可変ＤＮＳレコードのセットは、ドメイン・ネームの所与の事例では、メール交換（ＭＸ）データ、テキスト（ＴＸＴ）データ、別名（ＣＮＡＭＥ）データ、もしくは他の種類のデータに関連するデータである、またはそのいずれかを含むことができる。しかしながら、他の実装形態では、上記のタイプのデータ（ＭＸなど）が、ゾーン・ファイル１１６に格納された可変回答情報に組み込み可能であり、かつ／または他の情報が、非可変ＤＮＳレコード１１８に格納可能であることが理解されよう。

【００２５】

問合せ１０４が１０６で受信されると、データが、１１６および１０８から検索され、またポリシー・サーバ１０８を使用してゾーン・ファイル１１６から検索される回答１１４または回答１１４の構成要素を選択するために使用される。代わりに、またはさらに、データを１１８から検索することができる。１１６および／または１１８から検索されたデータは、署名付きの回答１２０内で連結し、符号化することができ、署名付きの回答は

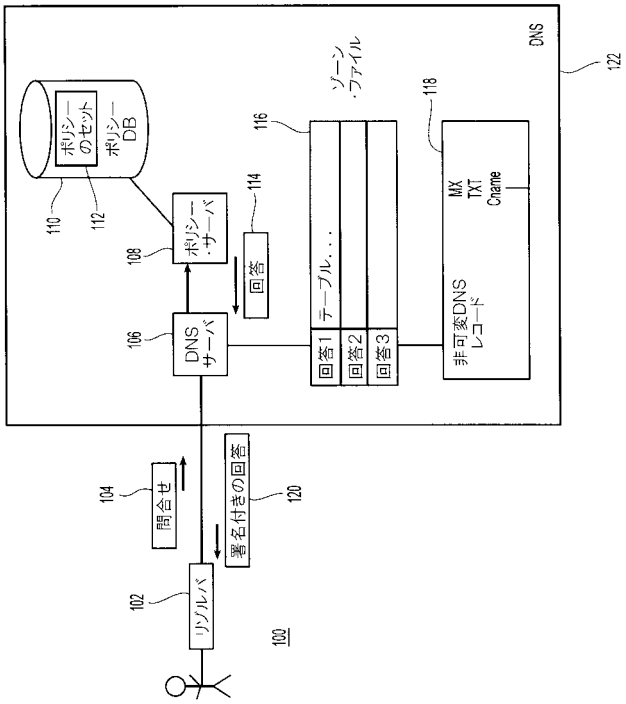
、リゾルバ１０２に返される。
【００２６】
図２は、ゾーン・ファイル１１６で使用可能な例示的なデータ構造を示す。図に示すような実装形態では、ゾーン・ファイル１１６は、ゾーン・ファイル１１６のテーブル・ストアへのキーもしくは索引として使用可能な可変ＩＤ１２４を含む様々な情報を符号化し、または格納することができる。所有者名、クラス、タイプ、レコード・データ（ＲＤＡＴＡ）、開始、および有効期限などの他の情報は、ゾーン・ファイル１１６内に記録することができる。ゾーン・ファイル１１６はまた、可変ＩＤ１２４によって識別される各可変回答に関連する鍵データに基づく署名１２６を含むことができる。署名１２６は、署名付きの回答１２０が本物であり、信頼できることを保証するよう、公開鍵情報を使用して、リゾルバ１０２または他のユーザによって検査することができる。次いで、回答自体、または回答の署名１２６を生成する必要なく、自発的またはオンザフライで、署名付きの回答１２０を検索し、リゾルバ１０２に送信することができる。
【００２７】
図３は、各態様による、レコード・セットへのＤＮＳＳＥＣ対応ゾーンの事前署名を行うためのシステムおよび方法で実行可能なポリシー調整、署名付きデータの経路生成、ならびに他の処理の流れ図を示す。３０２では、処理を開始できる。３０４では、ＤＮＳ１２２は、所与のゾーンまたは対象となるゾーンに対して、ポリシーのセット１１２に基づいて変動する、または異なるポリシー依存のレコードを識別することができる。３０６では、ＤＮＳ１２２は、ポリシーのセット１１２の適用によって生み出された各可変レコード・セットのために、考え得るすべての値を定義する、または生成することができる。３０８では、ＤＮＳ１２２は、ポリシーのセット１１２から各可変回答を選択するのに使用する１つまたは複数のポリシーを識別することができる。
【００２８】
３１０では、ＤＮＳ１２２は、ポリシーのセット１１２によって生み出された各可変回答を含むゾーン・ファイル１１６に個々に署名することができる。ゾーン・ファイル１１６への署名は、オフラインでアクセスされる鍵データ、すなわち、専用の鍵データ・ストレージ・システム、または他の記憶装置もしくはホストを含む別個のシステムに格納されている鍵データを使用して実現される。３１２では、ＤＮＳ１２２は、リゾルバ１０２から、ＩＰアドレスを求める要求などの問合せ１０４、および／または他のクエリもしくは要求を受信することができる。３１４では、問合せ１０４がＤＮＳ１２２によって（非可変ＤＮＳレコード１１８ではなく）可変リソース・レコード・セットを要求していると判定された場合、ＤＮＳ１２２は、ポリシーのセット１１２において、関連する１つまたは複数のポリシーを呼び出して、署名付きの回答１２０を選定または選択することができる。３１６では、ＤＮＳ１２２は、選択された１つまたは複数のポリシーに基づいて、署名付きの回答１２０をリゾルバ１０２に返すことができる。３１８では、処理は、繰返し、前の処理ポイントへの復帰、さらなる処理ポイントへのジャンプ、または終了が可能である。
【００２９】
図４は、各実装形態による、ＤＮＳ１２２に組み込み可能な様々なハードウェア、ソフトウェア、および他のリソースを示す。図に示すような実装形態において、ＤＮＳ１２２は、電子的なランダム・アクセス・メモリなどのメモリ１４２と通信する、またオペレーティング・システム１４６の制御下でもしくはオペレーティング・システム１４６と共に動作するプロセッサ１４０を含むプラットフォームを備えることができる。実装形態におけるプロセッサ１４０は、１つまたは複数のサーバ、クラスタ、および／または他のコンピュータもしくはハードウェア・リソースに組み込み可能であり、かつ／またはクラウドベースのリソースを使用して実現することができる。オペレーティング・システム１４６は、例えば、Ｌｉｎｕｘ（登録商標）オペレーティング・システム、Ｕｎｉｘ（登録商標）オペレーティング・システム、または他のオープンソースもしくはベンダー独自のオペレーティング・システムもしくはプラットフォームのディストリビューションであっても

よい。プロセッサ１４０は、ローカル・ハード・ドライブまたはドライブ・アレイに格納されたデータベースなどのデータストア１４８と通信し、ゾーン・ファイル１１６もしくは複数のゾーン・ファイル、他のＤＮＳレコード、および／またはそれらの選択によるサブセット、ならびに他のコンテンツ、メディア、または他のデータへのアクセスあるいはその格納を行うことができる。プロセッサ１４０は、Ｅｔｈｅｒｎｅｔ（登録商標）または無線データ接続などのネットワーク・インターフェース１５０とも通信することができ、ネットワーク・インターフェース１５０はさらに、インターネットまたは他のパブリック／プライベート・ネットワークなどの１つまたは複数のネットワーク１５２と通信する。プロセッサ１４０は、概して、制御論理を実行するように、またＤＮＳ１２２の制御下で、ＤＮＳ運用に関係する問合せ１０４、ポリシーのセット１１２、ＩＰアドレス情報、および／または他のデータもしくは情報を処理することを含む様々な処理動作を制御するように、プログラムする、あるいは構成することができる。各態様では、リゾルバ１０２、および対象となるドメインの任意のゾーン・サーバは、ＤＮＳ１２２のリソースに類似したリソースである、もしくはそれらを含むことができ、かつ／または追加のもしくは異なるハードウェア、ソフトウェア、および／または他のリソースを含むことができる。ＤＮＳ１２２、リゾルバ１０２、関連するネットワーク接続、ならびに他のハードウェア、ソフトウェア、およびサービス・リソースの他の構成も可能である。

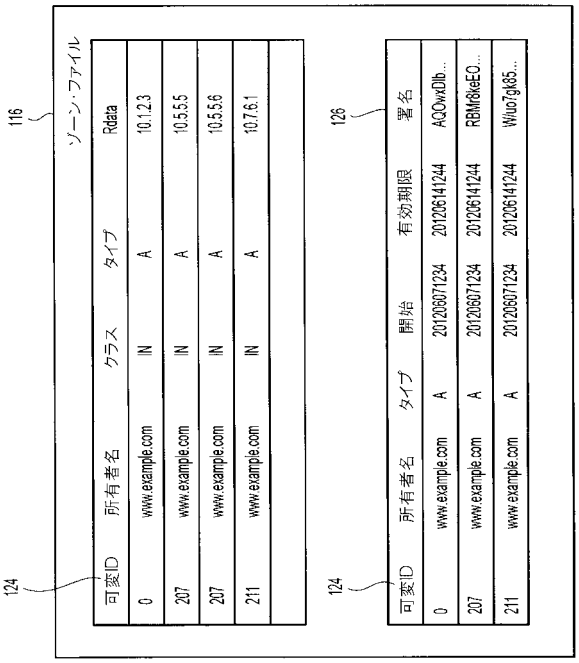
【００３０】

以上の説明は例示的なものであり、当業者であれば、構成および実装の変形形態を思いつくであろう。例えば、ＤＮＳ１２２の１つのプラットフォームまたは要素が所与のドメインをサポートする実装形態が説明されてきたが、各実装形態では、ドメインをサポートするために、２つ以上のドメイン・ネーム・システム（ＤＮＳ）を展開することができる。単数または統合型として説明された他のリソースは、実装形態において、複数または分散型である場合があり、また複数または分散型として説明されたリソースは、実装形態において、組み合わされている場合がある。それゆえに、本教示の範囲は、添付の特許請求の範囲によってのみ限定されるものである。

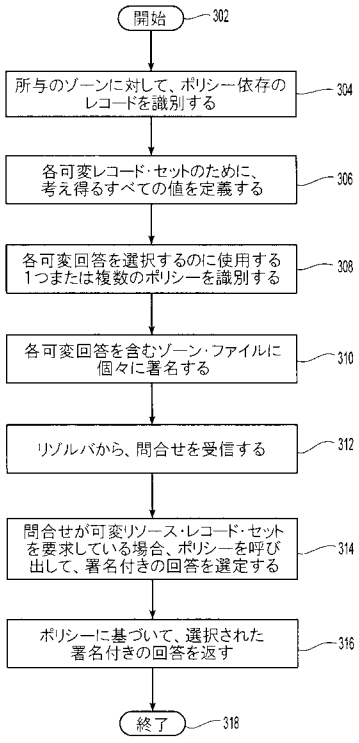
【図１】


DNS
122
ポリシー
のセット
ポリシー
DB
110
112
ポリシー
・サーバ
108
114
回答
ゾーン
・ファイル
116
テーブル...
回答1
回答2
回答3
118
MX
TXT
Cname
非可変DNS
レコード
DNS
サーバ
106
問合せ
104
署名付きの回答
120
リゾルバ
102
100

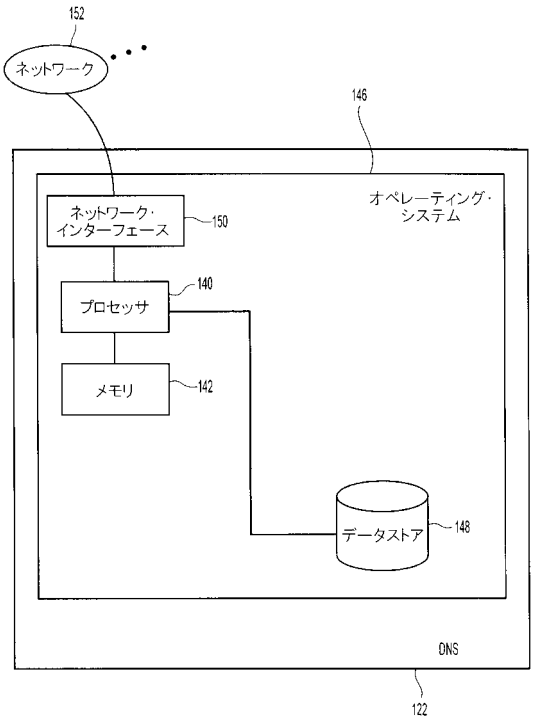
【図２】


116
ゾーン・ファイル
可変ID
所有者名
クラス
タイプ
Rdata
0
www.example.com
IN
A
10.1.2.3
207
www.example.com
IN
A
10.5.5.5
207
www.example.com
IN
A
10.5.5.6
211
www.example.com
IN
A
10.7.6.1
124
126
可変ID
所有者名
タイプ
開始
有効期限
署名
0
www.example.com
A
20120606071234
20120614141244
AQOwsDlb...
207
www.example.com
A
20120606071234
20120614141244
RBM6keEO...
211
www.example.com
A
20120606071234
20120614141244
Wiuo7gk85...

【図３】


開始
302
所与のゾーンに対して、ポリシー依存の
レコードを識別する
304
各可変レコード・セットのために、
考え得るすべての値を定義する
306
各可変回答を選択するのに使用する
1つまたは複数のポリシーを識別する
308
各可変回答を含むゾーン・ファイルに
個々に署名する
310
リゾルバから、問合せを受信する
312
問合せが可変リソース・レコード・セット
を要求している場合、ポリシーを呼び
出して、署名付きの回答を選定する
314
ポリシーに基づいて、選択された
署名付きの回答を返す
316
終了
318

【図４】


152
ネットワーク
146
オペレーティング・
システム
ネットワーク・
インターフェース
150
プロセッサ
140
メモリ
142
データストア
148
DNS
122

フロントページの続き

(72)発明者　デーヴィッド　ブラッカ
アメリカ合衆国　２０１９０　ヴァージニア　レストン　ブルーモント　ウェイ　１２０６１　シー／オー　ベリサイン　リーガル　デパートメント
(72)発明者　ラマカント　パンドランギ
アメリカ合衆国　２０１９０　ヴァージニア　レストン　ブルーモント　ウェイ　１２０６１　シー／オー　ベリサイン　リーガル　デパートメント

Ｆターム(参考) 5B084 AA22 AB04 AB30 BB16 DB02 DC02

【外国語明細書】
2014182828000001.pdf