IBM Systems - iSeries

ネットワーキング
DNS (Domain Name System)

バージョン 5 リリース 4

IBM

IBM Systems - iSeries

ネットワーキング
DNS (Domain Name System)

バージョン 5 リリース 4

お願い

本書および本書で紹介する製品をご使用になる前に、 43 ページの『特記事項』に記載されている情報をお読みください。

本書は、IBM i5/OS (プロダクト番号 5722-SS1) のバージョン 5、リリース 4、モディフィケーション 0 に適用されます。また、改訂版で断りがない限り、それ以降のすべてのリリースおよびモディフィケーションにも適用されます。このバージョンは、すべての RISC モデルで稼働するとは限りません。また、CISC モデルでは稼働しません。

本マニュアルに関するご意見やご感想は、次の URL からお送りください。今後の参考にさせていただきます。

http://www.ibm.com/jp/manuals/main/mail.html

なお、日本 IBM 発行のマニュアルはインターネット経由でもご購入いただけます。詳しくは

http://www.ibm.com/jp/manuals/ の「ご注文について」をご覧ください。

(URL は、変更になる場合があります)

お客様の環境によっては、資料中の円記号がバックスラッシュと表示されたり、バックスラッシュが円記号と表示されたりする場合があります。

原　典： IBM Systems - iSeries
Networking
Domain Name System
Version 5 Release 4

発　行： 日本アイ・ビー・エム株式会社

担　当： ナショナル・ランゲージ・サポート

第1刷 2006.2

この文書では、平成明朝体™W3、平成明朝体™W7、平成明朝体™W9、平成角ゴシック体™W3、平成角ゴシック体™W5、および平成角ゴシック体™W7を使用しています。この(書体*)は、(財) 日本規格協会と使用契約を締結し使用しているものです。フォントとして無断複製することは禁止されています。

注* 平成明朝体™W3、平成明朝体™W7、平成明朝体™W9、平成角ゴシック体™W3、
平成角ゴシック体™W5、平成角ゴシック体™W7

© Copyright International Business Machines Corporation 1998, 2006. All rights reserved.

© Copyright IBM Japan 2006

目次

© Copyright IBM Corp. 1998, 2006

DNS

ドメイン・ネーム・システム (DNS) は、ホスト名およびそれに関連するインターネット・プロトコル (IP) アドレスを管理するための分散データベース・システムです。

DNS を使用すると、ユーザーは、ホストを見つけるのに、IP アドレス xxx.xxx.xxx.xxx ではなく、簡単な名前、たとえば www.jkltoys.com などを使用できます。1 つのサーバーが 1 つのゾーンの小さなサブセットのホスト名と IP アドレスがわかっていれば、 DNS サーバーが協同で作業を行ってすべてのドメイン・ネームをそれぞれの IP アドレスにマップすることができます。協同する DNS サーバーは、コンピューターがインターネットを通じて通信できるようにするサーバーです。

IBM® OS/400® バージョン 5 リリース 1 (V5R1) の場合、DNS サービスは Berkeley Internet Name Domain (BIND) バージョン 8 と呼ばれる業界標準による DNS インプリメンテーションを基にしています。前の IBM OS/400 DNS サービスは、BIND バージョン 4.9.3 を基にしていました。 新しい BIND バージョン 8 ベースの DNS サーバーを使用するには、 i5/OS™ オプション 33、ポータブル・アプリケーション・ソリューション環境 (PASE) が、IBM eServer™ iSeries™ サーバーにインストールされていなければなりません。 PASE がインストールされていない場合でも、以前のリリースで使用可能だった同じ DNS サーバー (BIND 4.9.3 ベース) を継続して実行することができます。 ただし、BIND 8 にマイグレーションすると、改良された機能が提供され、DNS サーバーのセキュリティーも改良されます。

注: このトピックでは、BIND 8 を基にした新規機能について説明します。 BIND 8 ベースの DNS を実行するのに必要な PASE を使用しない場合は、BIND 4.9.3 ベースの DNS について、『V4R5 DNS Information Center』トピックを参照してください。

印刷可能 PDF

本書の PDF を表示およびプリントするには、以下の説明を使用してください。

本書の PDF バージョンを表示あるいはダウンロードするには、「ドメイン・ネーム・システム」を選択します。

PDF ファイルの保管

表示用または印刷用の PDF ファイルをワークステーションに保存するには、次のようにします。

1. ブラウザーで PDF ファイルを右マウス・ボタンでクリックする (上記のリンクを右マウス・ボタンでクリックする)。
2. PDF をローカルで保管するオプションをクリックする。
3. PDF ファイルを保管する先のディレクトリーを指定する。
4. 「**保管**」をクリックする。

Adobe Reader のダウンロード

これらの PDF を表示または印刷するには、システムに Adobe Reader がインストールされていることが必要です。Adobe Web サイト (www.adobe.com/products/acrobat/readstep.html) から、無償コピーをダウンロードできます。

© Copyright IBM Corp. 1998, 2006

ドメイン・ネーム・システムの概念

このトピックでは、ドメイン・ネーム・システム (DNS) とは何か、どのような働きをするのかについて説明します。また、1 つの DNS サーバー上で定義できるさまざまなタイプのゾーンについても説明します。

ドメイン・ネーム・システム (DNS) は、ホスト名およびそれに関連するインターネット・プロトコル (IP) アドレスを管理するための分散データベース・システムです。 DNS を使用すると、ユーザーは、ホストを見つけるのに、IP アドレス xxx.xxx.xxx.xxx ではなく、簡単な名前、たとえば www.jkltoys.com などを使用できます。 1 つのサーバーが 1 つのゾーンの小さなサブセットのホスト名と IP アドレスがわかっていれば、 DNS サーバーが協同で作業を行ってすべてのドメイン・ネームをそれぞれの IP アドレスにマップすることができます。協同する DNS サーバーは、コンピューターがインターネットを通じて通信できるようにするサーバーです。

DNS データは、ドメイン階層に分解されます。サーバーは、単一のサブドメインなどのデータのほんの一部分を知っているだけです。そのサーバーが直接管理する必要があるドメイン部分はゾーンと呼ばれます。あるゾーンについて完全なホスト情報とデータを持っている DNS サーバーは、そのゾーンの権限サーバーです。権限サーバーは、そのゾーン内のホストに関する照会に、独自のリソース・レコードを使用して応答することができます。その照会プロセスは、複数の要素により決まります。『DNS 照会について』には、照会に応答するためにクライアントが使用できるパスについての説明があります。

ゾーンについて

このトピックでは、ドメイン・ネーム・システム (DNS) のゾーンおよびゾーンのタイプについて説明します。

DNS データは、ゾーンと呼ばれる管理可能なデータのセットに分割されます。ゾーンには、1 つの DNS ドメインの一部または複数部分に関する名前および IP アドレスが含まれています。1 つのゾーンに対する情報すべてを含んだサーバーは、そのドメインに対する権限サーバーです。場合によっては、特定のサブドメインに関する DNS 照会の応答権限を、別の DNS サーバーに代行させることは意味のあることです。この場合、そのドメインに対する DNS サーバーはそのサブドメイン照会が該当のサーバーを参照するように構成することができます。

障害時のバックアップと冗長性を考慮して、ゾーン・データは権限 DNS サーバー以外のサーバー上に格納するのが普通です。この別サーバーは 2 次サーバーと呼ばれ、権限サーバーからゾーン・データをロードします。2 次サーバーを構成することにより、サーバーにかかる要求をバランスできるようになるとともに、1 次サーバー・ダウン時のバックアップを提供できるようにもなります。2 次サーバーは、権限サーバーからのゾーン転送によってゾーン・データを入手します。 2 次サーバーは、初期化時に 1 次サーバーからゾーン・データの完全コピーをロードします。また、2 次サーバーは、ゾーン・データが変更されると、1 次サーバーかまたは該当ドメイン用の他の 2 次サーバーからゾーン・データを再ロードします。

DNS ゾーン・タイプ

iSeries DNS を使用して、以下に示すいくつかのゾーン・タイプを定義し、DNS データの管理に役立てることができます。

1 次ゾーン

1 次ゾーンは、ホスト上のファイルから直接ゾーン・データをロードします。 1 次ゾーンにはサブゾーンまたは子ゾーンを入れることができます。また、1 次ゾーンには、リソース・レコード (ホスト、別名 (CNAME)、アドレス (A)、または逆マッピング・ポインター (PTR) レコードなど) を入れることもできます。

注: 1 次ゾーンは、他の BIND 資料で マスター・ゾーン と呼ばれる場合があります。

サブゾーン

サブゾーンは 1 次ゾーン内のゾーンを定義します。サブゾーンにより管理可能な断片にゾーン・データを編成できるようにします。

子ゾーン

子ゾーンはサブゾーンを定義し、サブゾーン・データに対する責任を 1 つまたは複数のネーム・サーバーに代行させます。

別名 (CNAME)

別名は、1 次ドメイン・ネームに対する代替名を定義します。

ホスト

ホスト・オブジェクトは、A と PTR レコードをホストにマッピングします。追加のリソース・レコードを、ホストに関連付けることができます。

2 次ゾーン

2 次ゾーンは、ゾーン・データを、ゾーンの 1 次サーバーまたは別の 2 次サーバーからロードします。 2 次サーバーは、そのゾーン・データがセカンダリーとなるゾーンの完全コピーを管理します。

スタブ・ゾーン

スタブ・ゾーンは、2 次ゾーンに似ていますが、そのゾーンのネーム・サーバー (NS) レコードだけを転送します。

フォワード・ゾーン

フォワード・ゾーンは、その特定ゾーンあてのすべての照会を他のサーバーに転送します。

関連概念

『DNS 照会について』
このトピックでは、DNS がクライアントに代わって照会を解決する方法について説明します。

28 ページの『ネーム・サーバー上のゾーンの構成』
DNS サーバー・インスタンスを構成したら、 次に、ネーム・サーバーのゾーンを構成する必要があります。

関連資料

14 ページの『例: イントラネット用単一 DNS サーバー』
この例は、内部使用のための DNS サーバーを持った単純なサブネットを示します。

8 ページの『DNS リソース・レコード』
このトピックでは、DNS によるリソース・レコードの使用方法が説明されています。リソース・レコードは、ドメイン・ネームと IP アドレスに関するデータを格納するのに使用されます。このトピックには、 OS/400 V5R1 でサポートされるリソース・レコードの検索可能リストが含まれています。

DNS 照会について

このトピックでは、DNS がクライアントに代わって照会を解決する方法について説明します。

クライアントは DNS サーバーを使用して、そのサーバーから情報を見付けます。 その要求はクライアントから直接入ってくることも、クライアント上で実行中のアプリケーションから入ってくることもあります。クライアントは照会メッセージを DNS サーバーに送信します。そのメッセージには、完全修飾のドメイン・ネーム (FQDN)、照会タイプ (クライアントが必要とする特定のリソース・レコードなど)、およびドメイン・ネームのクラス (通常、インターネット (IN) クラス) が含まれます。次の図には、インターネット・アクセスを行う単一 DNS サーバーのサンプル・ネットワークが示されています。

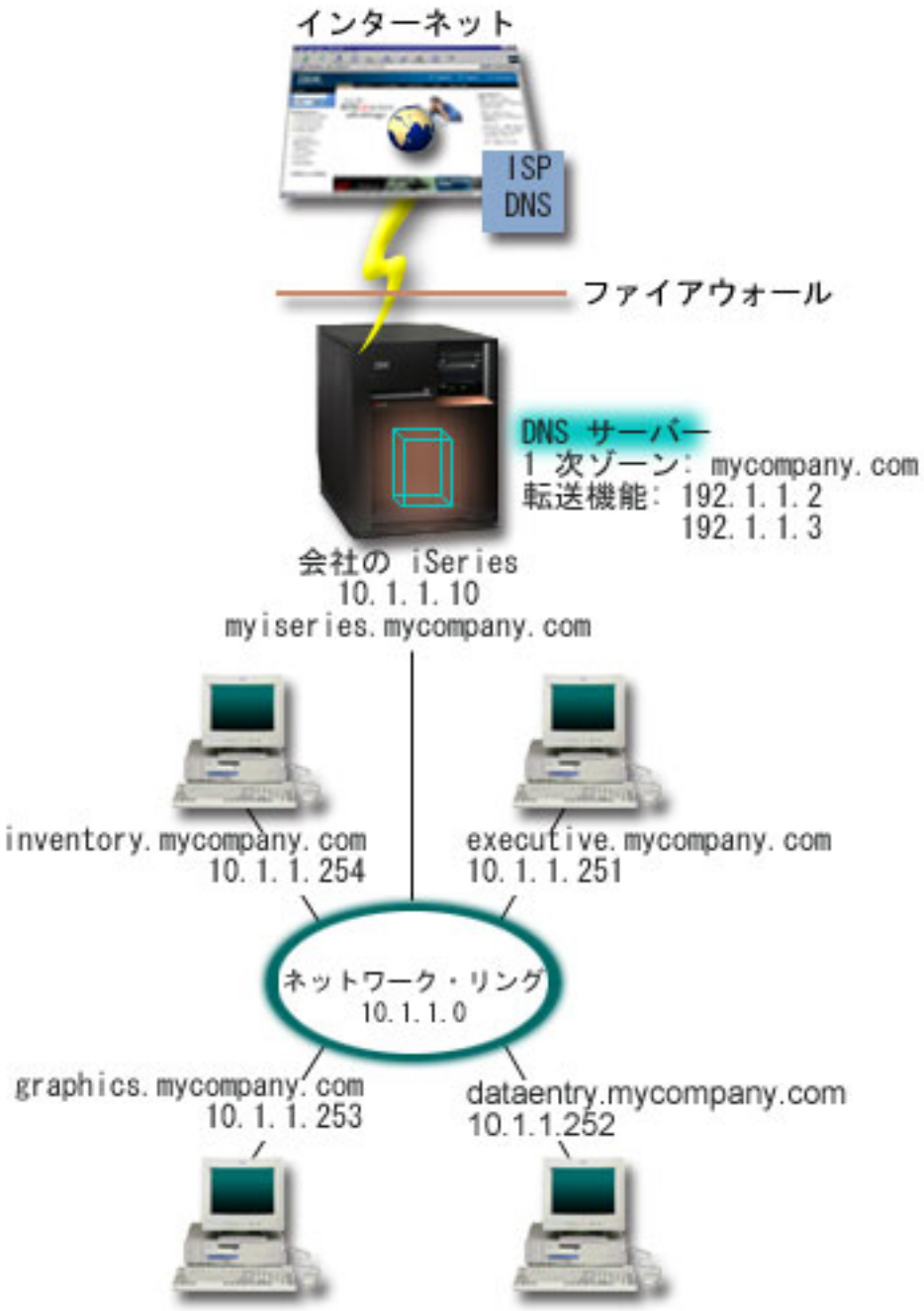

図 1. インターネット・アクセスを行う単一 DNS サーバー

ホスト *dataentry* は 「graphics.mycompany.com」に関して DNS サーバーに照会すると仮定します。 DNS サーバーは自分自身が持っているゾーン・データを使用して、IP アドレス 10.1.1.253 で応答します。

次に、*dataentry* は、「www.jkl.com.」の IP アドレスを要求するとします。このホストは、この DNS サーバーのゾーン・データ内にはありません。たどれる経路には、再帰または反復の 2 つがあります。DNS サーバーは、再帰を使用するように設定されている場合、このサーバーは、要求側のクライアントに代わって名前を完全に解決するために他の DNS サーバーに照会または連絡してからクライアントに回答を戻します。 DNS サーバーが別の DNS サーバーに照会する場合、要求側のサーバーは応答をキャッシュに入れておき、次回照会を受けたときにその応答を使えるようにします。クライアントは、自分自身で名前を解決す

るために、他の DNS サーバーに連絡してみることができます。反復 と呼ばれるこのプロセスでは、クライアントは、サーバーからの参照応答に基づいて、別個の追加照会を使用します。

関連資料

2 ページの『ゾーンについて』
このトピックでは、ドメイン・ネーム・システム (DNS) のゾーンおよびゾーンのタイプについて説明します。

16 ページの『例: インターネット・アクセスを行う単一 DNS サーバー』
この例は、インターネットに直接接続されている DNS サーバーを持った単純なサブネットを示します。

DNS ドメインのセットアップ

このトピックには、ドメイン登録の概要と、ユーザー自身のドメイン・スペースをセットアップする際に必要なその他の参照サイトへのリンクについての説明があります。

DNS により、イントラネットまたは内部ネットワーク上の名前とアドレスを提供できるようになります。また、DNS により、インターネット経由で、世界中に名前とアドレスを提供できるようになります。インターネット上にドメインをセットアップする場合、ドメイン・ネームを登録することが必要です。

イントラネットを設定している場合、内部使用のためにドメイン・ネームを登録する必要はありません。イントラネット名を登録するかどうかは、内部的な使用とは関係なく、インターネット上でその名前を誰も使用できないようにしたいかどうかに依存します。内部的に使用する予定の名前を登録すると、後でそのドメイン・ネームを外部的に使用する場合に、競合が起こりません。

ドメイン登録は、許可されたドメイン・ネーム登録機関に直接連絡して行うか、インターネット・サービス・プロバイダー (ISP) を介して行います。一部の ISP では、ドメイン・ネーム登録要求を代行して依頼するサービスを提供しています。 Internet Network Information Center (InterNIC) では、Internet Corporation for Assigned Names and Numbers (ICANN) で許可されているすべてのドメイン・ネーム登録機関のディレクトリーを管理しています。

関連資料

16 ページの『例: インターネット・アクセスを行う単一 DNS サーバー』
この例は、インターネットに直接接続されている DNS サーバーを持った単純なサブネットを示します。

関連情報

Internet Network Information Center (InterNIC)

動的更新

OS/400 V5R1 DNS (BIND 8 ベース) は、動的更新をサポートします。これにより、DHCP などの外部ソースが DNS サーバーに更新を送信できるようになります。

DHCP は、中央サーバーを使用して、ネットワーク全体の IP アドレスおよび他の構成の詳細を管理する TCP/IP 規格です。 DHCP サーバーはクライアントからの要求に応答し、クライアントにプロパティーを動的に割り当てます。 DHCP により、中央でネットワーク・ホスト構成パラメーターを定義し、ホストの構成を自動化できます。 DHCP を使用して、使用可能な IP アドレス数よりも多くのクライアントを持ったネットワーク用に、一時的 IP アドレスをクライアントに割り当てることがあります。

過去には、すべての DNS データは静的なデータベースに格納されていました。すべての DNS リソース・レコードの作成と維持管理は、管理者が行わなければなりませんでした。現在では、BIND 8 で稼働する DNS サーバーはゾーン・データを動的に更新する他ソースからの要求を受け入れるように構成されています。

ご使用の DHCP サーバーを構成して、ホストに新しいアドレスが割り当てられるたびに、DNS サーバーに更新要求を送信することができます。この自動化されたプロセスにより、TCP/IP ネットワークの急速な増大または変更に関する DNS サーバーの管理作業を軽減します。ホスト・ロケーションが頻繁に変更されるネットワークでも同様です。 DHCP を使用しているクライアントが IP アドレスを受信すると、そのアドレスは即時に DNS サーバーに送信されます。この方式を使用することにより、IP アドレスが変更された場合でも、DNS は正確にホストへの照会を解決し続けることができます。

DHCP を構成して、アドレスのマッピング (A) レコード、逆検索ポインター (A) レコード、またはその両方を、クライアントに代わって更新できます。A レコードはマシンのホスト名をその IP アドレスにマッピングします。PTR レコードは、マシンの IP アドレスをそのホスト名にマッピングします。クライアントのアドレスが変更されると、DHCP は自動的に更新を DNS サーバーに送信します。それにより、ネットワーク中のホストがその新 IP アドレスで DNS 照会することにより、クライアントを見付けられるようにします。動的に更新される各レコードごとに、そのレコードが DHCP により作成されたことを示す関連テキスト (TXT) レコードが書き込まれます。

注: DHCP が PTR レコードのみを更新するように設定されている場合、各クライアントがその A レコードを更新できるように、クライアントからの更新を可能にするように DNS を構成する必要があります。 すべての DHCP クライアントが、自分自身の A レコードの更新要求を行うことをサポートするとは限りません。この方式を選択する前に、ご使用のクライアント・プラットフォームの資料を調べてください。

更新を送信可能な、許可されたソースのリストを作成することにより、動的ゾーンは保護されます。個々の IP アドレス、全サブネット、共有秘密鍵 (トランザクション・シグニチャー または TSIG と呼ばれる) を使用してサインされたパケット、またはこれらの方式の組み合わせを使用して、許可されたソースを定義できます。 DNS は、送られてくる要求パケットが許可されたソースから来ていることをリソース・レコードの更新前に検証します。

動的更新は、単一 iSeries サーバー上の DNS と DHCP の間、異なる iSeries サーバー間、または iSeries と、動的更新が可能なその他のサーバーとの間で実行できます。

注: 動的更新 API QTOBUPT は、動的更新を DNS に送信するサーバー上に必要です。これは、i5/OS オプション 31 の DNS では自動的にインストールされます。

関連概念

動的ホスト構成プロトコル (DHCP)

関連タスク

28 ページの『動的更新を受信するための DNS の構成』
BIND 8 で実行される DNS サーバーは、 ゾーン・データを動的に更新する他ソースからの要求を受け入れるように構成することができます。 このトピックでは、allow-update オプションの構成手順を説明します。 それにより、DNS が動的更新を受信できるようになります。

動的更新を送信するための DHCP の構成

関連資料

18 ページの『例: DNS と DHCP が同一 iSeries サーバーにある場合』
この例は、DNS と DHCP が同一サーバーにある場合を示します。

8 ページの『DNS リソース・レコード』
このトピックでは、DNS によるリソース・レコードの使用方法が説明されています。リソース・レコードは、ドメイン・ネームと IP アドレスに関するデータを格納するのに使用されます。このトピックには、 OS/400 V5R1 でサポートされるリソース・レコードの検索可能リストが含まれています。

QTOBUPT

『BIND 8 機能』
動的更新以外に、BIND 8 は、ご使用の DNS サーバーの性能を向上するいくつかの機能を提供しています。

BIND 8 機能

動的更新以外に、BIND 8 は、ご使用の DNS サーバーの性能を向上するいくつかの機能を提供しています。

DNS は、OS/400 V5R1 の BIND 8 を使用するように再設計されました。 PASE がインストールされていない場合は、前にリリースされた (BIND 4.9.3 ベースの) OS/400 DNS サーバーを引き続き構成し実行できます。 DNS のシステム要件に関するトピックには、 iSeries サーバーで BIND 8 ベースの DNS を実行するために必要なことがらについての説明があります。新 DNS の使用により、以下の機能を利用できるようになります。

単一 iSeries 上での複数 DNS サーバーの稼働

前のリリースでは、1 つの DNS サーバーだけを構成することができました。このリリースから、複数の DNS サーバーまたはインスタンスを構成できるようになりました。これによって、サーバー間に論理的な仕切りをセットアップできるようになります。複数インスタンスを作成する場合、各インスタンスごとに明示的に listen-on インターフェース IP アドレスを定義する必要があります。 2 つの DNS インスタンスは同一インターフェースで listen できません。

複数サーバーの実用的なアプリケーションは、分割 DNS です。分割 DNS では、1 つの権限サーバーが内部ネットワークを管理し、2 番目のサーバーが外部からの照会に使用されます。

条件付き転送

条件付き転送により、転送プリファレンスを細かくチューニングするように DNS サーバーを構成できます。サーバーに回答がわからない、すべての照会を転送するようにサーバーを設定できます。グローバル・レベルで転送を設定できますが、通常の反復による解決を強制したいドメインには、例外を追加することもできます。または、グローバル・レベルで通常の反復による解決を設定してから、特定のドメイン内で転送を強制することもできます。

動的更新の保護

動的ホスト構成プロトコル (DHCP) およびその他の許可ソースは、トランザクション・シグニチャー (TSIG) またはソース IP アドレス許可 (あるいはその両方) を使用して、動的リソース・レコード更新を送信できます。これにより、許可されたソースだけを更新に使用することが保証されると同時に、手動によるゾーン・データ更新作業が減少します。

NOTIFY

NOTIFY がオンになっていると、1 次サーバー上でゾーン・データが更新される時はいつも DNS NOTIFY 通知機能がアクティブになります。 1 次サーバーは、データが変更された旨のメッセージを、管理下のすべての 2 次サーバーに送信します。次いで、2 次サーバーは、更新済みゾーン・データを求めるゾーン転

送要求を出して応答します。これにより、バックアップ・ゾーン・データを最新状態に保持することができ、2 次サーバーのサポートを向上します。

ゾーン転送 (IXFR および AXFR)

以前では、2 次サーバーがゾーン・データの再ロードを必要とする時はいつも、2 次サーバーは、完全なデータ・セット自体をすべてのゾーン転送 (AXFR) でロードする必要がありました。BIND 8 では、新ゾーン転送方式をサポートします。それが増分ゾーン転送 (IXFR) です。IXFR は、他サーバーがゾーンを丸ごと転送する代わりに、変分データのみを転送できる方式です。

この方式が 1 次サーバーで使用可能になると、データ変更には、変更がある旨のフラグが割り当てられます。2 次サーバーがゾーン更新を IXFR 方式で要求した場合、1 次サーバーは新しいデータのみを送信します。 IXFR がとくに便利なのは、ゾーンが動的に更新される場合です。この転送方式を使用すれば、より少ない量のデータを送信することによって、トラフィック負荷を減らせます。

注: この機能を使用するには、1 次サーバーと 2 次サーバーの両方で IXFR が使用可能になっている必要があります。

関連概念

25 ページの『DNS の要件』
このトピックでは、iSeries サーバーで DNS を実行するためのソフトウェア要件について説明します。

5 ページの『動的更新』
OS/400 V5R1 DNS (BIND 8 ベース) は、動的更新をサポートします。これにより、DHCP などの外部ソースが DNS サーバーに更新を送信できるようになります。

関連資料

20 ページの『例: ファイアウォールでの分割 DNS』
この例では、ファイアウォールを通して作動する DNS を示します。 これにより、内部データはインターネットから保護されますが、内部ユーザーはインターネット上のデータにアクセスできます。

23 ページの『セキュリティー基準の計画』
DNS には、いくつかのセキュリティー・オプションがあり、サーバーへの外部からのアクセスを制限します。

DNS リソース・レコード

このトピックでは、DNS によるリソース・レコードの使用方法が説明されています。リソース・レコードは、ドメイン・ネームと IP アドレスに関するデータを格納するのに使用されます。このトピックには、OS/400 V5R1 でサポートされるリソース・レコードの検索可能リストが含まれています。

DNS ゾーン・データベースはリソース・レコードの集まりで構成されています。各リソース・レコードには、特定オブジェクトに関する情報が指定されています。たとえば、アドレス・マッピング (A) レコードは、ホスト名を IP アドレスにマップし、逆検索ポインター (PTR) レコードは、IP アドレスをホスト名にマップします。 サーバーはこれらのレコードを使用して、そのゾーン内のホストあてに照会の応答を行います。詳しくは、以下の表を使用して DNS リソース・レコードを表示してください。

表 1. リソース・レコード参照表

リソース・レコード	省略形	説明
アドレス・マッピング・レコード (Address Mapping records)	A	A レコードは、このホストの IP アドレスを指定します。A レコードは、特定ドメイン・ネームの IP アドレスに関する照会を解決するために使用されます。このレコード・タイプは RFC (Request For Comments) 1035 で定義されます。
Andrew File System データベース・レコード (Andrew File System Database records)	AFSDB	AFSDB レコードは、オブジェクトの AFS® アドレスまたは DCE アドレスを指定します。AFSDB レコードは、A レコードのように使用され、ドメイン・ネームをその AFSDB アドレスにマップします。または、セルのドメイン・ネームから、そのセルの認証済みネーム・サーバーにマップします。このレコード・タイプは RFC 1183 で定義されます。
正規名レコード (Canonical Name records)	CNAME	CNAME レコードは、このオブジェクトの実際のドメイン・ネームを指定します。 DNS が別名を照会して、正規名を指す CNAME レコードを検出すると、DNS はその正規ドメイン・ネームを照会します。このレコード・タイプは RFC 1035 で定義されます。
ホスト情報レコード (Host Information records)	HINFO	HINFO レコードは、ホスト・マシンに関する一般情報を指定します。標準 CPU 名およびオペレーティング・システム名は Assigned Numbers RFC 1700 で定義されます。ただし、標準番号の使用は必須ではありません。このレコード・タイプは RFC 1035 で定義されます。
サービス総合ディジタル網レコード (Integrated Services Digital Network records)	ISDN	ISDN レコードは、このオブジェクトのアドレスを指定します。このレコードはホスト名を ISDN アドレスにマップします。このレコードは ISDN ネットワークでのみ使用されます。このレコード・タイプは RFC 1183 で定義されます。

表 1. リソース・レコード参照表 (続き)

リソース・レコード	省略形	説明
IP バージョン 6 アドレス・レコード (IP Version 6 Address records)	AAAA	AAAA レコードは、ホストの 128 ビット・アドレスを指定します。 AAAA レコードは A レコードのように使用され、ホスト名をその IP アドレスにマップします。 AAAA レコードは、標準の A レコード形式に適合しない IP バージョン 6 アドレスのサポートに使用してください。このレコード・タイプは RFC 1886 で定義されます。
ロケーション・レコード (Location records)	LOC	LOC レコードは、ネットワーク・コンポーネントの物理的なロケーションを指定します。このレコードは、ネットワーク効率の評価または物理ネットワークのマッピングを行うために、アプリケーションによって使用されます。このレコード・タイプは RFC 1876 で定義されます。
メール・エクスチェンジャー・レコード (Mail Exchanger records)	MX	MX レコードは、このドメインに送信されるメール用のメール・エクスチェンジャー・ホストを定義します。このレコードは、SMTP (Simple Mail Transfer Protocol) によって使用され、このドメインのメールの処理または転送を行うホストを見付けるために各メール・エクスチェンジャー・ホストのプリファレンス値と一緒に使用されます。各メール・エクスチェンジャー・ホストには、有効なゾーン内に対応するホスト・アドレス (A) レコードが必要です。このレコード・タイプは RFC 1035 で定義されます。
メール・グループ・レコード (Mail Group records)	MG	MG レコードは、メール・グループ・ドメイン・ネームを指定します。このレコード・タイプは RFC 1035 で定義されます。
メールボックス・レコード (Mailbox records)	MB	MB レコードは、このオブジェクト用のメールボックスを含むホスト・ドメイン・ネームを指定します。このドメインに送信されるメールは、MB レコードで指定されたホストに送信されます。このレコード・タイプは RFC 1035 で定義されます。

表 1. リソース・レコード参照表 (続き)

リソース・レコード	省略形	説明
メールボックス情報レコード (Mailbox Information records)	MINFO	MINFO レコードは、このオブジェクトに関するメッセージまたはエラーを受信するメールボックスを指定します。 MINFO レコードは、単一のメールボックスよりも、メーリング・リストによく使用されます。このレコード・タイプは RFC 1035 で定義されます。
メールボックス名前変更レコード (Mailbox Rename records)	MR	MR レコードは、メールボックスの新しいドメイン・ネームを指定します。 MR レコードは、別のメールボックスに移動したユーザー用の転送項目として使用してください。このレコード・タイプは RFC 1035 で定義されます。
ネーム・サーバー・レコード (Name Server records)	NS	NS レコードは、このホストの権限ネーム・サーバーを指定します。このレコード・タイプは RFC 1035 で定義されます。
ネットワーク・サービス・アクセス・プロトコル・レコード (Network Service Access Protocol records)	NSAP	NSAP レコードは、NSAP リソースのアドレスを指定します。 NSAP レコードは、ドメイン・ネームを NSAP アドレスにマップするために使用されます。このレコード・タイプは RFC 1706 で定義されます。
公開鍵レコード (Public Key records)	KEY	KEY レコードは、DNS 名に関連付けられる公開鍵を指定します。この鍵は、ゾーン、ユーザー、またはホスト用のいずれでもかまいません。このレコード・タイプは RFC 2065 で定義されます。
責任者レコード (Responsible Person records)	RP	RP レコードは、このゾーンまたはホストの責任者のインターネット・メール・アドレスと記述を指定します。このレコード・タイプは RFC 1183 で定義されます。
逆検索ポインター・レコード (Reverse-lookup Pointer records)	PTR	PTR レコードは、PTR レコードが定義されるホストのドメイン・ネームを指定します。 IP アドレスがあれば、PTR レコードにより、ホスト名の検索が可能になります。このレコード・タイプは RFC 1035 で定義されます。

表 1. リソース・レコード参照表 (続き)

リソース・レコード	省略形	説明
ルート・スルー・レコード (Route Through records)	RT	RT レコードは、このホストのために IP パケットの転送機能の役目をするホスト・ドメイン・ネームを指定します。このレコード・タイプは RFC 1183 で定義されます。
権限開始レコード (Start of Authority records)	SOA	SOA レコードは、このサーバーをこのゾーンの権限サーバーとして指定します。権限サーバーはゾーン内で最良のデータ・ソースです。 SOA レコードには、ゾーンに関する一般情報と、2 次サーバーの再ロード規則が含まれます。存在できる SOA レコードは 1 ゾーンに 1 つです。このレコード・タイプは RFC 1035 で定義されます。
テキスト・レコード (Text records)	TXT	TXT レコードは、ドメイン・ネームに関連付けられる複数のテキスト・ストリングを指定します。各ストリングの長さは最大 255 文字です。 TXT レコードを責任者 (RP) レコードと一緒に使用すると、ゾーンの責任者がだれであるかの情報を提供することができます。このレコード・タイプは RFC 1035 で定義されます。 TXT レコードは、 iSeries DHCP で、動的更新のために使用されます。DHCP サーバーは、DHCP サーバーが PTR レコードおよび A レコードの更新を行うたびに、関連した TXT レコードを書き込みます。 DHCP レコードには AS400 DHCP という接頭部が付きます。
ウェルノウン・サービス・レコード (Well-Known Services records)	WKS	WKS レコードは、オブジェクトがサポートするウェルノウン・サービスを指定します。多くの場合、WKS レコードは、このアドレスに tcp と udp のいずれか、またはこの両方のプロトコルがサポートされていることを示します。このレコード・タイプは RFC 1035 で定義されます。
X.400 アドレス・マッピング・レコード (X.400 Address Mapping records)	PX	PX レコードは、X.400/RFC 822 マッピング情報を指すポインターです。このレコード・タイプは RFC 1664 で定義されます。

表 1. リソース・レコード参照表 (続き)

リソース・レコード	省略形	説明
X25 アドレス・マッピング・レコード (X25 Address Mapping records)	X25	X25 レコードは、X25 リソースのアドレスを指定します。このレコードはホスト名を PSDN アドレスにマップします。このレコードは X25 ネットワークでのみ使用されます。このレコード・タイプは RFC 1183 で定義されます。

関連概念

5 ページの『動的更新』
OS/400 V5R1 DNS (BIND 8 ベース) は、動的更新をサポートします。これにより、DHCP などの外部ソースが DNS サーバーに更新を送信できるようになります。

『メールおよびメール・エクスチェンジャー・レコード』
DNS は、 メールおよびメール・エクスチェンジャー (MX) レコードを使用した拡張メール・ルーティングをサポートしています。

関連資料

14 ページの『例: イントラネット用単一 DNS サーバー』
この例は、内部使用のための DNS サーバーを持った単純なサブネットを示します。

2 ページの『ゾーンについて』
このトピックでは、ドメイン・ネーム・システム (DNS) のゾーンおよびゾーンのタイプについて説明します。

メールおよびメール・エクスチェンジャー・レコード

DNS は、メールおよびメール・エクスチェンジャー (MX) レコードを使用した拡張メール・ルーティングをサポートしています。

メールおよび MX レコードは、Simple Mail Transfer Protocol (SMTP) などのメール・ルーティング・プログラムによって使用されます。 DNS リソース・レコードの中のルックアップ・テーブルには、iSeries DNS がサポートしているタイプのメール・レコードが入っています。

DNS には、メール・エクスチェンジャー情報を使用して、電子メールを送信するための情報が含まれています。ネットワークが DNS を使用している場合は、SMTP アプリケーションは TEST.IBM.COM への TCP 接続をオープンし、ホストの TEST.IBM.COM あてのアドレスにメールを配信するわけではありません。 SMTP はまず最初に、DNS サーバーに照会して、メッセージを配信するのに使用できるホスト・サーバーを見付けます。

特定アドレスへのメール配信

DNS サーバーは メール・エクスチェンジャー (MX) レコードと呼ばれるリソース・レコードを使用します。 MX レコードは、ドメインまたはホスト名をプリファレンス値とホスト名にマッピングします。 MX レコードは、通常、1 つのホストが別ホストあてのメールを処理するのに使用されるよう指定するのに使用されます。このレコードはまた、最初のホストにメールが届かなかった場合、別ホストにメールを配信するよう指定するのにも使用されます。言い換えれば、このレコードにより、あるホストあてのメールが別ホストあてに配信できるようになります。

複数 MX リソース・レコードは同一ドメインまたは同一ホスト名に対して存在する場合があります。複数 MX リソース・レコードが同一ドメインまたは同一ホスト名に対して存在している場合、各レコードのプリファレンス (または優先) 値が配信を試行する順序を決定します。最も低いプリファレンス値は、最優先レコードに関連し、最初にそのレコードが試行されます。最優先ホストにメールが届かない場合、メール送信アプリケーションは、次の優先 MX ホストにコンタクトしようとします。ドメイン管理者、または MX レコード作成者がプリファレンス値を設定します。

DNS サーバーは、その名前が DNS サーバーで権限を付与されているが、それに MX レコードが割り当てられていない場合、MX リソース・レコードの空リストで応答します。この状態が発生すると、メール送信アプリケーションは宛先ホストと直接接続を確立しようとします。

注: ドメイン用の MX レコードで、ワイルドカード (例 : `*.mycompany.com`) を使用することはお勧めできません。

例 : ホスト用の MX レコード

以下の例では、システムは、プリファレンス指定により、fsc5.test.ibm.com あてのメールをそのホスト自身に配信します。そのホストにメールが届かなかった場合、システムはメールを psfred.test.ibm.com または mvs.test.ibm.com (psfred.test.ibm.com にも届かなかった場合) に配信します。この例は、MX レコードがどのように指定されるかを示しています。

```
fsc5.test.ibm.com   IN MX 0 fsc5.test.ibm.com
                    IN MX 2 psfred.test.ibm.com
                    IN MX 4 mvs.test.ibm.com
```

関連資料

8 ページの『DNS リソース・レコード』
このトピックでは、DNS によるリソース・レコードの使用方法が説明されています。リソース・レコードは、ドメイン・ネームと IP アドレスに関するデータを格納するのに使用されます。このトピックには、 OS/400 V5R1 でサポートされるリソース・レコードの検索可能リストが含まれています。

DNS の例

以下に示す例を使用して、ご使用のネットワークで DNS をどのように使用できるかをご検討ください。

DNS は、ホスト名およびその関連 IP アドレスを管理するための分散データベース・システムです。以下の例は、DNS の機能およびご使用のネットワーク上でそれを使用可能にする方法を説明するのに有効です。この例には、そのセットアップおよび使用される理由が説明されています。各例には、その図を理解するのに有効と思われる関連概念へのリンクがあります。

例: イントラネット用単一 DNS サーバー

この例は、内部使用のための DNS サーバーを持った単純なサブネットを示します。

次の図は、iSeries 上で稼働する内部ネットワーク用の DNS です。 この単一 DNS サーバー・インスタンスは、全インターフェースの IP アドレス上で照会を listen するようにセットアップされています。このサーバーは「mycompany.com」ゾーン用の 1 次ネーム・サーバーです。

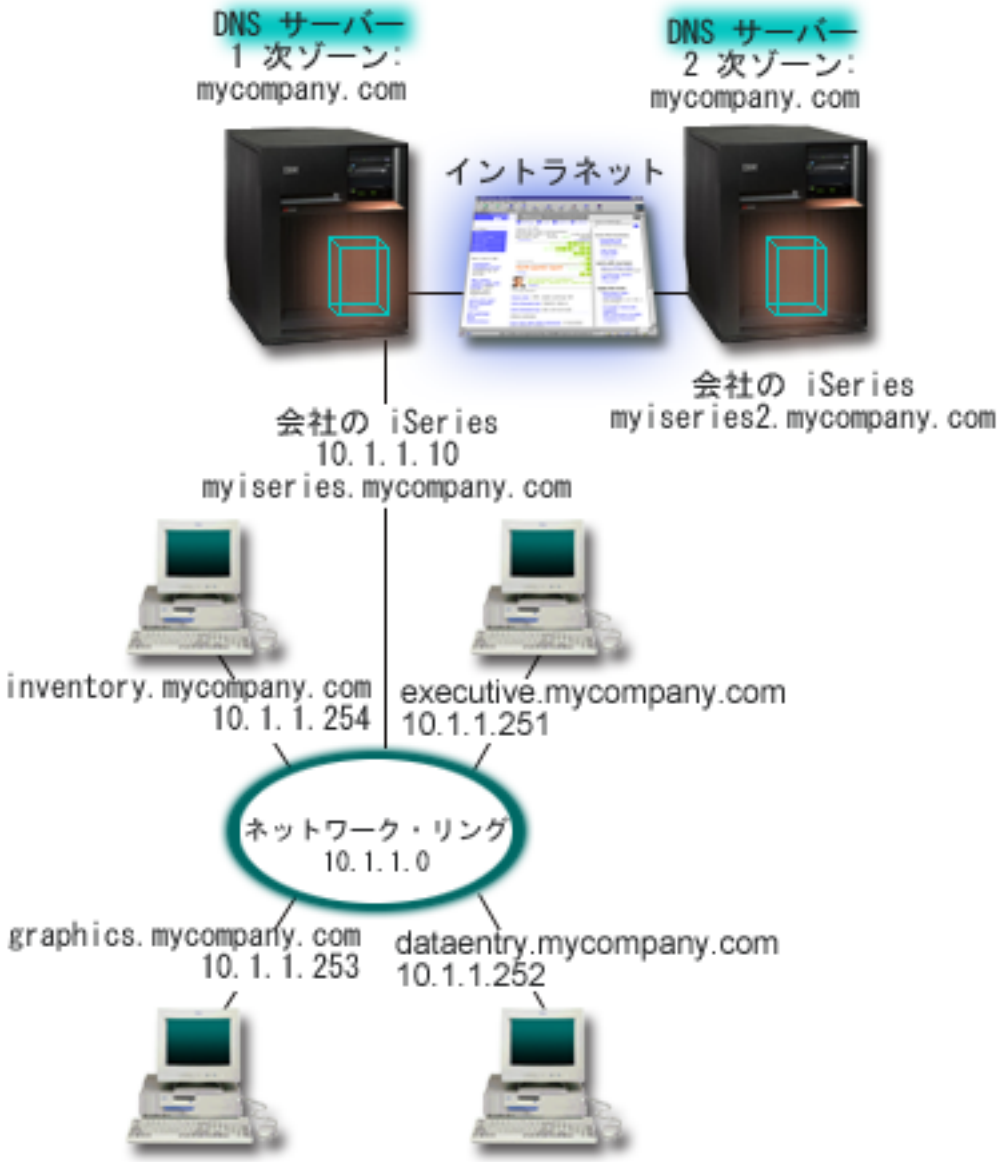

図 2. イントラネット用の単一 DNS サーバー

ゾーン内の各ホストには、IP アドレスとドメイン・ネームが付いています。管理者は、リソース・レコードを作成することにより、手動で DNS ゾーン・データにホストを定義する必要があります。アドレス・マッピング (A) レコードは、マシンの名前をその関連 IP アドレスにマップします。これにより、ネットワーク上の他のホストが DNS サーバーに照会して、特定ホスト名に割り当て済みの IP アドレスを見付けることができるようになります。逆検索ポインター (PTR) レコードは、マシンの IP アドレスをその関連ホスト名にマップします。これにより、ネットワーク上の他のホストが DNS サーバーに照会して、IP アドレスに対応するホスト名を見付けることができるようになります。

A および PTR レコードに加えて、DNS は多くの必要な他のリソース・レコードをサポートします。これは、ご使用のイントラネット上で稼働する TCP/IP ベースの他アプリケーションが何であるかにより異なります。たとえば、内部的な E-mail システムを実行している場合、メール・エクスチェンジャー (MX) レコードを追加する必要があります。それによって SMTP は、どのシステムがメール・サーバーを実行しているかを見付けるために DNS に照会することができます。

この小規模のネットワークが、より大規模なイントラネットの一部の場合、内部的なルート・サーバーを定義する必要があります。

2 次サーバー

2 次サーバーはゾーン・データを権限サーバーからロードします。2 次サーバーは、権限サーバーからのゾーン転送によってゾーン・データを入手します。 2 次ネーム・サーバーが始動すると、このサーバーは指定ドメインあての全データを 1 次サーバーから要求します。 2 次ネーム・サーバーは、1 次サーバーに更新済みデータを要求します。その理由は、2 次ネーム・サーバーが 1 次ネーム・サーバーから通知を受信したか (NOTIFY 機能が使用されている場合)、1 次ネーム・サーバーに照会した結果、データが変更されていることが判明したか、のいずれかです。図 2 では、サーバー「myiseries」はイントラネットの一部です。もう 1 つの iSeries サーバー「myiseries2」は、mycompany.com ゾーン用の 2 次 DNS サーバーとして機能するように構成されています。 2 次 DNS サーバーを使用して、サーバーにかかる要求をバランスさせることができます。また、1 次サーバー障害時のバックアップとしても使用することができます。各ゾーンごとに最低 1 つの 2 次サーバーを持つことが、実質的に有効です。

関連資料

8 ページの『DNS リソース・レコード』
このトピックでは、DNS によるリソース・レコードの使用方法が説明されています。リソース・レコードは、ドメイン・ネームと IP アドレスに関するデータを格納するのに使用されます。このトピックには、 OS/400 V5R1 でサポートされるリソース・レコードの検索可能リストが含まれています。

2 ページの『ゾーンについて』
このトピックでは、ドメイン・ネーム・システム (DNS) のゾーンおよびゾーンのタイプについて説明します。

『例: インターネット・アクセスを行う単一 DNS サーバー』
この例は、インターネットに直接接続されている DNS サーバーを持った単純なサブネットを示します。

例: インターネット・アクセスを行う単一 DNS サーバー

この例は、インターネットに直接接続されている DNS サーバーを持った単純なサブネットを示します。

次の図では、イントラネット用の単一 DNS サーバーの例と同じネットワーク例を図示していますが、ここでは、インターネットへの接続を追加しました。この例では、この会社はインターネットにアクセスすることができますが、この会社のネットワークへのインターネット・トラフィックは、ファイアウォールによりブロックされるように構成されています。

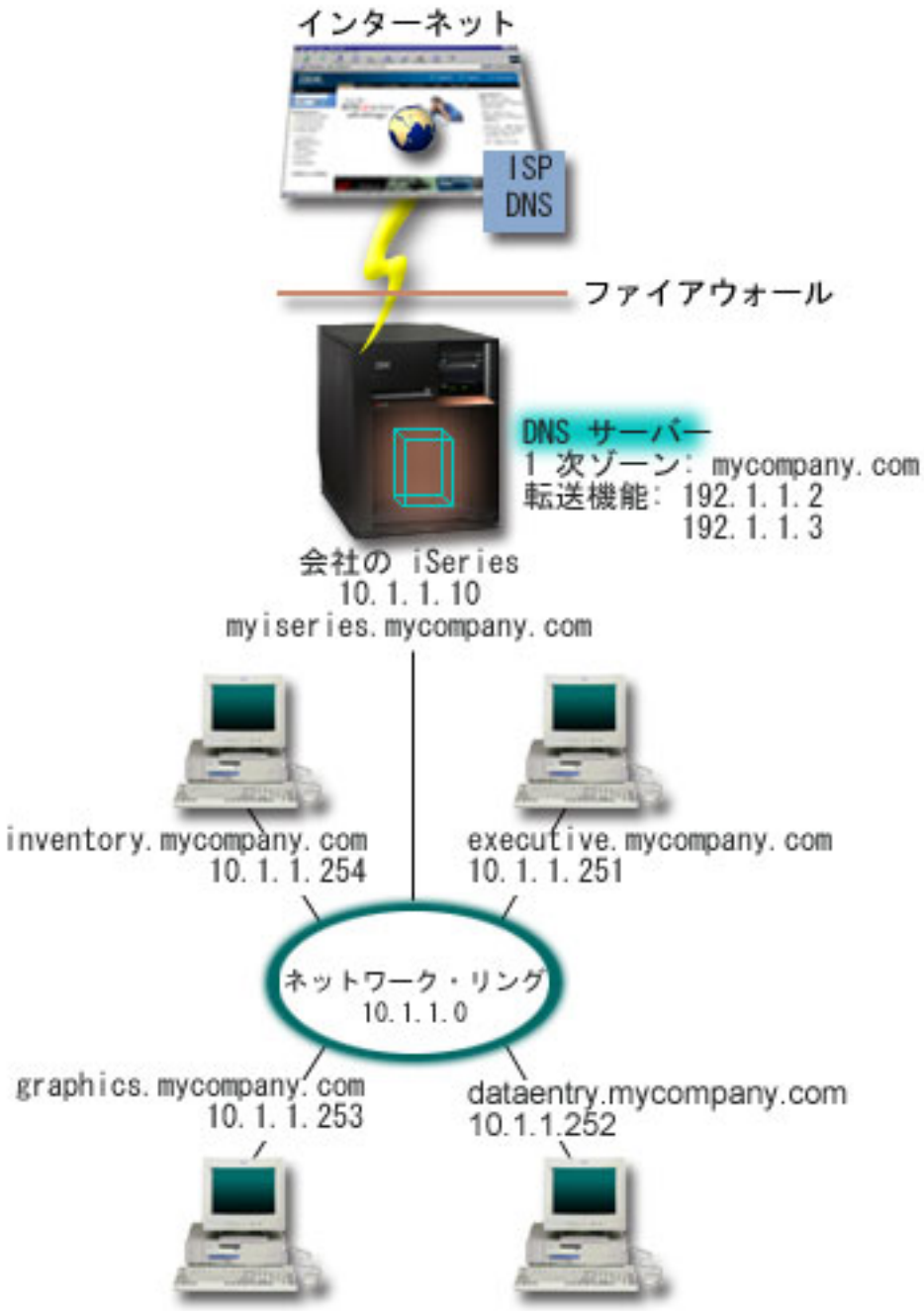

図 3. インターネット・アクセスを行う単一 DNS サーバー

IP アドレスを解決するには、以下の作業の少なくとも 1 つを実行する必要があります。

- インターネット・ルート・サーバーの定義

  デフォルトのインターネット・ルート・サーバーを自動的にロードできますが、そのリストを更新する必要があります。これらのサーバーは、ユーザー自身のゾーン外のアドレスを解決するのに役立ちます。現行のインターネット・ルート・サーバーを入手する方法については、 30 ページの『外部 DNS データのアクセス』を参照してください。
- 転送の使用可能化

mycompany.com のゾーン外のアドレス照会を、外部の DNS サーバー (インターネット・サービス提供者 (ISP) が運用している DNS サーバーなど) に渡すように転送をセットアップすることができます。転送方式およびルート・サーバー方式の両方による検索を使用可能にしたい場合、forward オプションを **first** に設定する必要があります。このサーバーは最初に転送方式を行い、そこで照会が解決ができなかった場合にルート・サーバーに照会します。

以下の構成変更も必要となる場合があります。

- 無制限の IP アドレス割り当て

  上記の例では、10.x.x.x のアドレスが示されています。しかし、これらは制約されたアドレスであり、イントラネット外では使用できません。このアドレスは、例示目的用に下に示されていますが、ユーザー自身の IP アドレスは ISP または他のネットワーキング要因によって決定されます。
- 自分のドメイン・ネームの登録

  インターネットからアクセスできる場合で、まだドメイン・ネームが登録されていない場合、ドメイン・ネームの登録を行う必要があります。
- ファイアウォールの確立

  ご使用の DNS がインターネットに直接接続されるようにすることはお勧めできません。ファイアウォールを構成するか、他の予防措置を講じてご使用の iSeries サーバーを保護してください。

関連概念

5 ページの『DNS ドメインのセットアップ』
このトピックには、ドメイン登録の概要と、 ユーザー自身のドメイン・スペースをセットアップする際に必要なその他の参照サイトへのリンクについての説明があります。

iSeries およびインターネット・セキュリティー

3 ページの『DNS 照会について』
このトピックでは、DNS がクライアントに代わって照会を解決する方法について説明します。

関連資料

14 ページの『例: イントラネット用単一 DNS サーバー』
この例は、内部使用のための DNS サーバーを持った単純なサブネットを示します。

例: DNS と DHCP が同一 iSeries サーバーにある場合

この例は、DNS と DHCP が同一サーバーにある場合を示します。

この構成は、DHCP が IP アドレスをホストに割り当てた場合に、DNS ゾーン・データを動的に更新するのに使用できます。

次の図では、4 つのクライアントに対して DNS と DHCP サーバーとして機能する 1 つの iSeries サーバーを持った、小規模のサブネット・ネットワークが図示されています。 この稼働環境で、在庫、データ入力、経営者の各クライアントがグラフィックス・ファイル・サーバーでグラフィックスの資料を作成すると仮定します。各クライアントは、そのホスト名に対するネットワーク・ドライブによりグラフィックス・ファイル・サーバーに接続します。

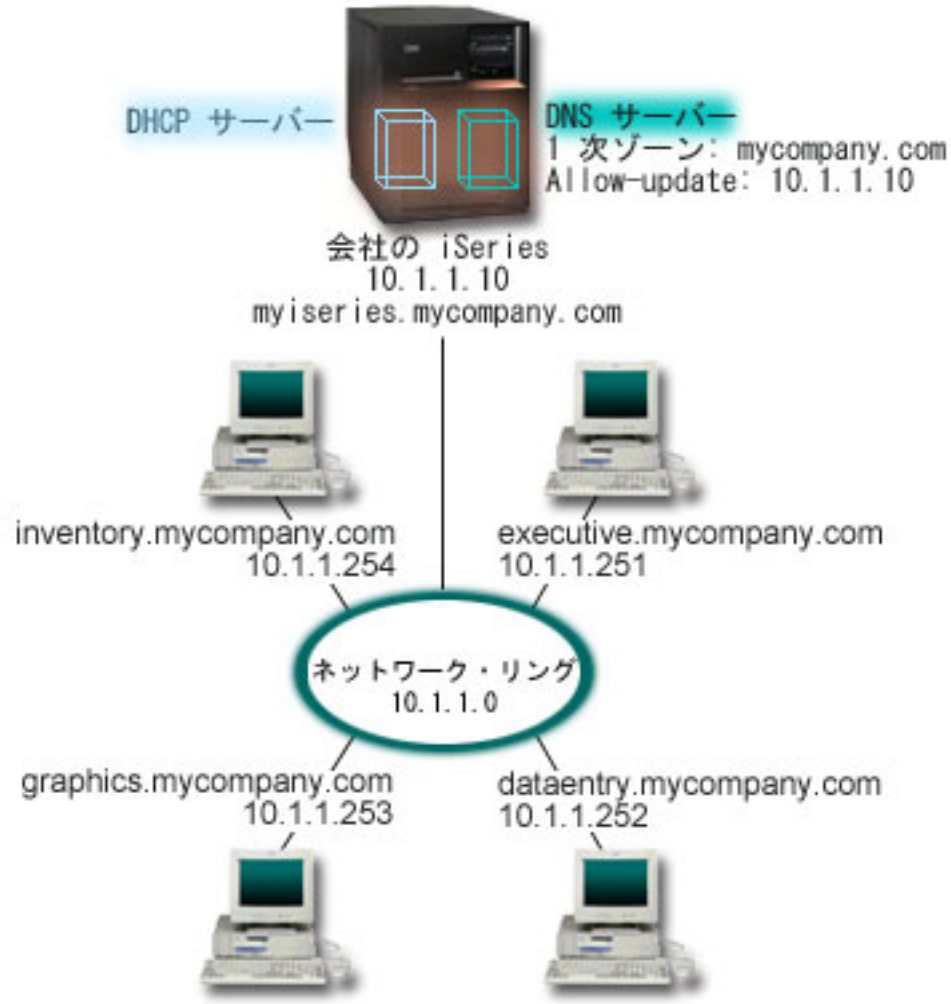

図 4. DNS と DHCP が同一 iSeries サーバーにある場合

以前のバージョンの DHCP と DNS はお互いに独立していました。 DHCP がクライアントに新しい IP アドレスを割り当てた場合、DNS レコードを管理者が手動で更新する必要がありました。この例では、グラフィックス・ファイル・サーバーの IP アドレスが DHCP により変更された場合、そこにアクセスするクライアントはネットワーク・ドライブをそのホスト名にマップできなくなります。理由は、DNS レコードが以前のファイル・サーバーの IP アドレスを持っているからです。

BIND 8 に基づく OS/400 V5R1 DNS サーバーでは、DHCP による断続的なアドレス変更と共に DNS レコードに対する動的更新を受け入れるように DNS ゾーンを構成することができます。たとえば、グラフィックス・ファイル・サーバーがそのリースを更改して、新たに IP アドレス 10.1.1.250 を DHCP が割り当てると、関連する DNS レコードは動的に更新されます。 これによりその他のクライアントが、グラフィックス・ファイル・サーバーについて、そのホスト名で、DNS サーバーに中断せずに照会できるようになります。

DNS ゾーンを構成して動的更新を受け入れるには、以下の作業を完了してください。

- 動的ゾーンの識別化

  サーバー稼働中は手動で動的ゾーンを更新することができません。それを行うと、送られてくる動的更新と干渉を起こします。手動による更新ができるのは、サーバーの停止後です。ただし、サーバー停止

中に送信された動的更新はすべて失われます。この理由により、手動による更新を最小限にするために、別の動的ゾーンを構成する必要が生じます。動的更新機能を使用するゾーンの構成について詳しくは、 23 ページの『ドメイン構造の決定』を参照してください。

- allow-update オプションの構成

  更新許可 (allow-update) オプションで構成されたすべてのゾーンは、動的ゾーンと考えられます。更新許可オプションはゾーン単位ベースで設定されます。動的更新を受け入れるには、更新許可オプションがこのゾーンで使用可能になっている必要があります。この例では、mycompany.com ゾーンは allow-update データを持っていますが、サーバー上に定義された他のゾーンは、静的または動的として構成できます。
- 動的更新を送信する DHCP 構成

  ご使用の DHCP サーバーによる、分散された IP アドレス用 DNS レコードの更新を許可する必要があります。
- 2 次サーバーの更新プリファレンスの構成

  2 次サーバーを最新状態に保つために、NOTIFY 機能を使用するように DNS を構成することができます。これはゾーン・データが変更されたときに mycompany.com ゾーン用の 2 次サーバーにメッセージを送信するためです。また、増分ゾーン転送 (IXFR) も構成する必要があります。これにより、IXFR 対応の 2 次サーバーが、ゾーン全体ではなく、更新されたゾーン・データのみをトラッキングしロードできるようになります。

DNS と DHCP を別々のサーバーで稼働させる場合は、DHCP サーバーに対していくつかの追加構成要件があります。

関連概念

5 ページの『動的更新』
OS/400 V5R1 DNS (BIND 8 ベース) は、動的更新をサポートします。これにより、DHCP などの外部ソースが DNS サーバーに更新を送信できるようになります。

23 ページの『ドメイン構造の決定』
初めてドメインをセットアップする場合、ゾーンの作成前にその要求とメインテナンスに対する計画が必要です。

関連タスク

動的更新を送信するための DHCP の構成

関連資料

例: DNS と DHCP が異なる iSeries サーバーにある場合

例: ファイアウォールでの分割 DNS

この例では、ファイアウォールを通して作動する DNS を示します。これにより、内部データはインターネットから保護されますが、内部ユーザーはインターネット上のデータにアクセスできます。

次の図には、セキュリティー用のファイアウォールを使用した単純なサブネット・ネットワークが図示されてます。 BIND 8 を基にした OS/400 V5R1 DNS では、1 つの iSeries 上に、複数の DNS サーバーをセットアップすることができます。 この企業には、予約済みの IP スペースを持った内部ネットワーク、および外部に対し使用可能なネットワークの外部セクションがあると仮定します。

この企業では、その内部クライアントが外部のホスト名を解決できるようにして、外部の人たちとメール交換できるようにしたいと考えています。この企業はまた、その内部リゾルバーが、内部ネットワーク範囲外

では利用不能な内部用だけのゾーンにアクセスできるようにしたいとも考えています。しかし、いかなる外側リゾルバーも内部ネットワークにはアクセスできないようにしたいと考えています。

これを行うために、この企業では 2 つの DNS サーバー・インスタンスを同一 iSeries サーバー上にセットアップします。 1 つはイントラネット用、もう 1 つはパブリック・ドメイン用です。 これを *分割 DNS* と呼びます。

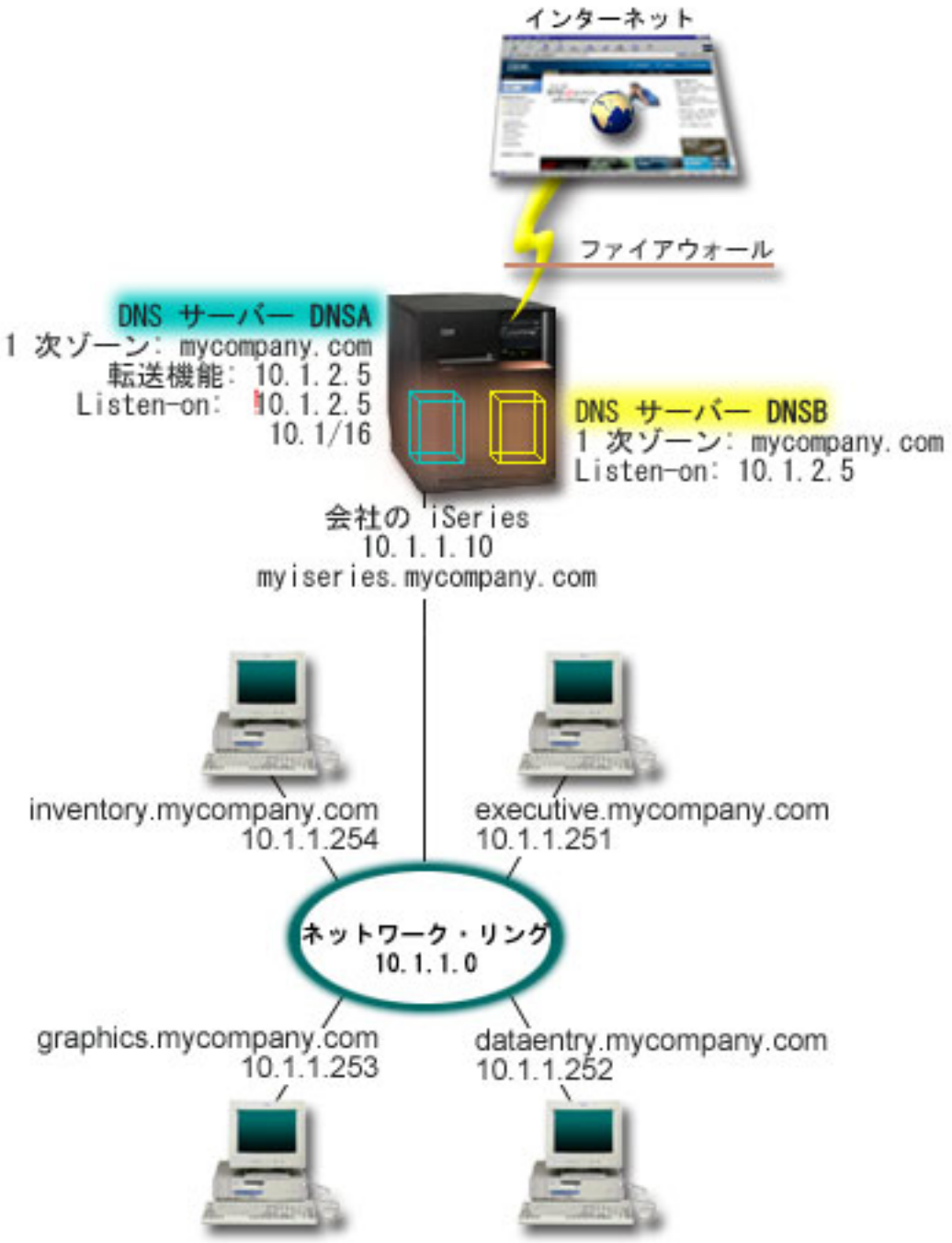

図 5. ファイアウォールを通した分割 DNS

外部サーバーの DNSB は、1 次ゾーン mycompany.com で構成されています。このゾーンのデータには、パブリック・ドメインの一部として意図されたリソース・レコードのみが含まれています。内部サーバーの

DNSA は、1 次ゾーン mycompany.com で構成されていますが、DNSA 上に構成されたゾーン・データにはイントラネット・リソース・レコードが含まれています。転送機能 (forwarders) オプションは 10.1.2.5 と定義されています。このオプションにより、DNSA が、自分で解決できないアドレス照会を DNSB に強制的に転送します。

ファイアウォールの保全または他のセキュリティーへの脅威が懸念される場合、内部データを保護するのに有効な listen-on オプションを使用する選択肢があります。これを行うためには、内部ホストから内部 mycompany.com ゾーンへ照会できるように、内部サーバーを構成することができます。これらすべてが正しく機能するには、内部クライアントは DNSA サーバーのみに照会するように構成する必要があります。分割 DNS をセットアップするには、以下の構成設定を考慮する必要があります。

- Listen-on

  前述の例では、iSeries 上には 1 つの DNS サーバーしかありませんでした。このサーバーは、すべてのインターフェース IP アドレスで listen するように設定されています。 1 つの iSeries 上に複数の DNS サーバーがある時はいつも、各サーバーが listen するインターフェース IP アドレスを定義する必要があります。 2 つの DNS サーバーが、同一アドレスで listen することはできません。この場合は、ファイアウォールから入ってくるすべての照会は、10.1.2.5 で送信されてくると仮定します。これらの照会は外部サーバーへ送信される必要があります。このため、DNSB は 10.1.2.5 で listen するように構成されます。内部サーバーの DNSA は、10.1.2.5 *以外* の 10.1.x.x 1 IP アドレスのいずれからでも、照会を受け入れるように構成されています。このアドレスを効率的に除外するには、アドレス・マッチ・リスト (AML) は、アドレス接頭部を組み込む前に、除外対象アドレスをリストしておく必要があります。

- アドレス・マッチ・リスト (AML) の順序

  指定されたアドレスと一致する AML 中の最初の要素が使用されます。たとえば、10.1.x.x ネットワーク上の 10.1.2.5 以外の全アドレスを許可するには、ACL 要素は (!10.1.2.5; 10.1/16) の順序になっている必要があります。この場合、アドレス 10.1.2.5 は最初の要素と比較されて、即時に否認されます。

  この要素が (10.1/16; !10.1.2.5) のように逆になっていると、IP アドレス 10.1.2.5 はアクセスを許可されます。理由は、サーバーはそのアドレスを最初の要素と比較し、それが一致すると残りのルールをチェックせずに許可するからです。

  関連資料

  7 ページの『BIND 8 機能』
  動的更新以外に、BIND 8 は、ご使用の DNS サーバーの性能を向上するいくつかの機能を提供しています。

DNS の計画

DNS は種々のソリューションを提供しています。DNS を構成する前に、ご使用のネットワーク内でどのように DNS を機能させるかを計画しておくことが重要です。ネットワーク構造、パフォーマンス、およびセキュリティーなどのサブジェクトを DNS をインプリメントする前に評価しておく必要があります。

DNS 権限の決定

DNS 管理者に対して特別な許可要件があります。許可が意味するセキュリティーについても検討する必要があります。

DNS セットアップ時にセキュリティー上の予防措置を講じて、ご使用の構成を保護します。どのユーザーが構成変更を許可されているかを設定する必要があります。

iSeries の管理者が、DNS の構成と管理を行うためには、最小レベルの権限が必要です。 すべてのオブジェクトのアクセス許可は、管理者が DNS 管理タスクを行うことができることを保証します。 DNS を構成するユーザーは、全オブジェクト (*ALLOBJ) 権限を持った機密保護担当者とすることをお勧めします。 iSeries ナビゲーターを使用して、ユーザーを許可してください。詳細が必要な場合、DNS オンライン・ヘルプにある「DNS 管理者への権限の付与」を参照してください。

注: 管理者のプロファイルに全権限がない場合、すべての DNS ディレクトリーと関連構成ファイルに対する特定のアクセスと権限が許可されている必要があります。

関連資料

33 ページの『DNS 構成ファイルの維持管理』
このトピックでは、DNS が使用するファイルについて理解していただくためと、 そのファイルをバックアップし維持管理するためのガイドラインを検討していただくための概要を説明します。

ドメイン構造の決定

初めてドメインをセットアップする場合、ゾーンの作成前にその要求とメインテナンスに対する計画が必要です。

ドメインまたはサブドメインをどのようにゾーン分割するか、ネットワーク要求を最良にサービスし、インターネットにアクセスするにはどうすればよいか、およびファイアウォールのネゴシエーションをどうするかを決定することは重要です。上記の要因は複雑であり、場合に応じて扱い方を代える必要があります。詳細なガイドラインとしては、「O'Reilly DNS and BIND」などの信頼できる情報源を参照してください。

動的ゾーンとして DNS ゾーンを構成する場合、サーバー稼働中は、手動によるゾーン・データへの変更はできません。それを行うと、送られてくる動的更新と干渉を起こします。手動による更新が必要な場合は、サーバーを停止し、変更を行ってからサーバーを再始動します。停止した DNS サーバーあてに送信された動的更新は失われます。この理由により、動的ゾーンと静的ゾーンを分離して構成する必要が生じます。これを行うには、動的に維持管理される予定のこれらのクライアントに対して、完全に分離したゾーンを作成するか、新規のサブドメイン (dynamic.mycompany.com など) を定義します。

iSeries DNS には、サーバーを構成するためのグラフィカル・インターフェースがあります。 ある場合には、このインターフェースは、他のソースとは異なる表現の用語または概念を使用する場合があります。DNS 構成の計画時に他の情報源を参照する場合、以下のことを知っていると便利です。

- サーバー内で定義されたすべてのゾーンとオブジェクトは、**前方参照ゾーン**と**逆引き参照ゾーン**というフォルダー内に構成されています。前方参照ゾーンはドメイン・ネームを IP アドレスにマッピング (A レコードなど) するのに使用するゾーンです。逆引き参照ゾーンは、IP アドレスをドメイン・ネームにマッピング (PTR レコードなど) するのに使用するゾーンです。
- iSeries DNS は、*1 次ゾーン* および *2 次ゾーン* を参照します。
- このグラフィカル・インターフェースでは サブゾーン という用語を使用しますが、一部の他情報源では、サブドメイン と呼ぶ場合があります。子ゾーンは、1 つまたは複数のネーム・サーバーにその責任が委任されたサブゾーンです。

関連資料

18 ページの『例: DNS と DHCP が同一 iSeries サーバーにある場合』
この例は、DNS と DHCP が同一サーバーにある場合を示します。

セキュリティー基準の計画

DNS には、いくつかのセキュリティー・オプションがあり、サーバーへの外部からのアクセスを制限します。

DNS サーバーを保護することは、最重要事項です。このトピックで説明するセキュリティー上の考慮事項以外に、 DNS セキュリティーおよび iSeries セキュリティーについては、Information Center にある「iSeries およびインターネット」などのさまざまなソースに説明があります。「DNS and BIND」という書籍も DNS に関連したセキュリティーを扱っています。

アドレス・マッチ・リスト

DNS はアドレス・マッチ・リストを使用して、一定の DNS 機能への外部エンティティー・アクセスを許可したり、拒否したりします。このリストには、特定の IP アドレス、サブネット (IP 接頭部を使用)、またはトランザクション・シグニチャー (TSIG) キーの使用を含むことができます。アドレス・マッチ・リストで、アクセスを許可または拒否したいエンティティーのリストを定義します。アドレス・マッチ・リストを再使用可能にしたい場合は、アクセス制御リスト (ACL) として保管することができます。そうすれば、このリストを提供する必要がある時はいつでも、ACL を呼び出して、その全リストをロードすることができます。

アドレス・マッチ・リスト要素の順序

指定されたアドレスと一致するアドレス・マッチ・リスト中の最初の要素が使用されます。たとえば、10.1.1.x ネットワーク上の 10.1.1.5 以外の全アドレスを許可するには、このマッチ・リストの要素は (!10.1.1.5; 10.1.1/24) の順序になっている必要があります。この場合、アドレス 10.1.1.5 は最初の要素と比較されて、即時に否認されます。

この要素が (10.1.1/24; !10.1.1.5) のように逆になっていると、IP アドレス 10.1.1.5 はアクセスを許可されてしまいます。理由は、サーバーはそのアドレスを最初の要素と比較し、それが一致すると残りのルールをチェックせずに許可してしまうからです。

アクセス制御オプション

DNS により、制約 (誰がサーバーへの動的更新を送信できるか、データを照会できるか、ゾーン転送を要求できるかなど) を設定することができるようになります。 ACL を使用して、サーバーへのアクセスを以下のオプションで制限することができます。

allow-update
ご使用の DNS サーバーが任意の外部ソースからの動的更新を受け入れるためには、allow-update オプションを使用可能にする必要があります。

allow-query
このサーバーへの照会を許可するホストを指定します。この指定がないと、デフォルトが適用され、全ホストからの照会が許可されます。

allow-transfer
このサーバーからのゾーン転送の受信を許可されるホストを指定します。この指定がないと、デフォルトが適用され、全ホストからの転送が許可されます。

allow-recursion
このサーバーを経由して再帰的照会を許可されるホストを指定します。この指定がないと、デフォルトが適用され、全ホストからの再帰的照会が許可されます。

blackhole
サーバーが照会の受け入れを拒否するか、または照会に対応するのに使用しないアドレスのリストを指定します。ここに指定されたアドレスからの照会は応答されません。

関連概念

iSeries およびインターネット・セキュリティー

関連資料

7 ページの『BIND 8 機能』
動的更新以外に、BIND 8 は、ご使用の DNS サーバーの性能を向上するいくつかの機能を提供しています。

DNS の要件

このトピックでは、iSeries サーバーで DNS を実行するためのソフトウェア要件について説明します。

DNS オプション (オプション 31) は基本オペレーティング・システムと一緒に自動インストールされません。インストール用に DNS を特定して選択する必要があります。OS/400 V5R1 用に追加された新規 DNS サーバーは、BIND 8 と呼ばれる業界標準の DNS インプリメンテーションを基にしています。前の OS/400 DNS サーバーは BIND 4.9.3 を基にしており、依然として OS/400 V5R1 で使用可能です。

DNS がインストールされると、デフォルトにより、以前のリリースで使用可能だった BIND 4.9.3 ベースの DNS サーバー機能を使用した単一 DNS サーバーをセットアップするように構成されます。 BIND 8 を使用した 1 つまたは複数の DNS サーバーを稼働したい場合は PASE をインストールする必要があります。 PASE は SS1 のオプション 33 です。PASE がインストールされると、iSeries ナビゲーターが、正しい BIND インプリメンテーションの構成作業を自動的に処理します。

PASE を使用しないと、BIND 8 の機能すべてを利用できるとは限りません。 PASE を使用しない場合、以前のリリースで使用可能だった DNS サーバー (BIND 4.9.3 ベース) と同じものを継続して実行することができます。 BIND 4.9.3 の資料については、V4R5 DNS Information Center トピックを参照してください。

別の iSeries に DHCP サーバーを構成して、この DNS サーバーに更新を送信するようにしたい場合は、オプション 31 も DHCP iSeries にインストールされていなければなりません。 DHCP サーバーは、オプション 31 によって提供されているプログラミング・インターフェースを使用して動的更新を実行します。

関連概念

Portable Application Solutions Environment (PASE)

26 ページの『DNS の構成』
このトピックでは、 iSeries ナビゲーターを使用して、ネーム・サーバーを構成し、自分以外のドメインで照会に応答する方法について説明します。

関連資料

7 ページの『BIND 8 機能』
動的更新以外に、BIND 8 は、ご使用の DNS サーバーの性能を向上するいくつかの機能を提供しています。

関連情報

V4R5 DNS Information Center トピック

DNS がインストールされているかどうかの判別

DNS がインストールされているかどうかを判別するには、以下のステップを実行します。

1. コマンド行で「`GO LICPGM`」と入力し、「Enter」を押します。
2. 「`10`」 (導入済みライセンス・プログラムの表示) と入力して、「Enter」を押します。
3. 「**5722SS1 ドメイン・ネーム・システム**」 (SS1 のオプション 31) までページダウンします。 DNS が正常にインストールされている場合、以下に示すように、「導入状況」が「`*compatible`」になります。

```
LicPgm     Installed Status     Description
5722SS1    *COMPATIBLE          Domain Name System
```

4. 「F3」を押して表示を終了します。

DNS のインストール

DNS をインストールするには、以下のステップを実行します。

1. コマンド行で「GO LICPGM」と入力し、「Enter」を押します。
2. 「11」 (ライセンス・プログラムの導入) と入力して「Enter」を押します。
3. Domain Name System の隣りの「**オプション**」フィールドに 1 (インストール) と入力して「Enter」を押します。
4. 「Enter」をもう一度押して、インストールを確認します。

DNS の構成

このトピックでは、 iSeries ナビゲーターを使用して、ネーム・サーバーを構成し、自分以外のドメインで照会に応答する方法について説明します。

DNS 構成を処理する前に、必要な DNS コンポーネントをインストールするための DNS システム要件を確認します。

関連概念

25 ページの『DNS の要件』
このトピックでは、iSeries サーバーで DNS を実行するためのソフトウェア要件について説明します。

iSeries ナビゲーターでの DNS のアクセス

このトピックでは、iSeries ナビゲーターで、DNS にアクセスする方法について説明します。

以下の手順では、iSeries ナビゲーターで、DNS 構成インターフェースに進みます。 PASE を使用している場合、BIND 8 に基づく DNS サーバーを構成することができます。 PASE を使用しない場合、以前のリリースで使用可能だった DNS サーバー (BIND 4.9.3 ベース) と同じものを継続して実行することができます。 BIND 4.9.3 ベースの DNS については、V4R5 DNS Information Center トピックを参照してください。

初めて DNS を構成する場合、以下の手順に従ってください。

1. iSeries ナビゲーターで、「**使用する iSeries サーバー** 」 → 「**ネットワーク**」 → 「**サーバー**」 → 「**DNS**」と展開します。
2. 「**DNS**」を右クリックし、「**新規構成**」を選択します。

関連概念

iSeries ナビゲーター

ネーム・サーバーの構成

DNS を使用すると、複数のネーム・サーバー・インスタンスを作成できます。このトピックではネーム・サーバーの構成手順を説明します。

BIND 8 ベースの iSeries DNS は、複数のネーム・サーバー・インスタンスをサポートします。以下に示す作業では、そのプロパティーおよびゾーンを含む単一ネーム・サーバー・インスタンスの作成のプロセスを行います。

複数インスタンスを作成したい場合、必要なすべてのインスタンスが作成されるまで、上記の手順を繰り返してください。各ネーム・サーバー・インスタンスごとに、デバッグ・レベルおよび自動開始値などの独立したプロパティーを指定することができます。新しいインスタンスが作成されると、個別の構成ファイルが作成されます。

関連資料

33 ページの『DNS 構成ファイルの維持管理』
このトピックでは、DNS が使用するファイルについて理解していただくためと、 そのファイルをバックアップし維持管理するためのガイドラインを検討していただくための概要を説明します。

ネーム・サーバー・インスタンスの作成

「新規 DNS 構成」ウィザードを使用して、DNS サーバー・インスタンスを定義します。

「**新規 DNS 構成**」ウィザードを開始するには、以下のステップに従ってください。

1. 「**iSeries ナビゲーター**」で、「**使用する iSeries サーバー**」 → 「**ネットワーク**」 → 「**サーバー**」 → 「**DNS**」と展開します。
2. 左側のペインで「**DNS**」を右クリックし、「**新規ネーム・サーバー**」を選択します。
3. このウィザードが構成プロセスをガイドします。

このウィザードには以下の入力が必要です。

DNS サーバー名:
DNS サーバーの名前を入力します。この名前は 5 文字までの長さで、英字で始まっている必要があります。複数サーバー作成時は、各名前は固有である必要があります。この名前は、システムの他のエリアで DNS サーバー「インスタンス」名と呼ばれます。

Listen-on IP アドレス:
2 つの DNS サーバーが、1 つの IP アドレスで listen することはできません。デフォルト設定では、すべての IP アドレスで listen します。追加のサーバー・インスタンスを作成する場合、どのサーバーも、すべてのアドレスで listen するように構成することはできません。各サーバーごとに IP アドレスを指定する必要があります。

ルート・サーバー:
デフォルトのインターネット・ルート・サーバーのリストをロードするか、イントラネット用の内部ルート・サーバーなど自分自身のルート・サーバーをロードします。

注: インターネットを使用していて、ご使用の DNS がインターネット名を完全に解決できることを期待している場合は、デフォルトのインターネット・ルート・サーバーだけをロードすることを考慮してください。

サーバーの開始:
TCP/IP の始動時に、サーバーが自動開始すべきかどうかを指定することができます。複数サーバーを稼働する場合、個々のインスタンスはお互いに無関係に開始および終了することができます。

DNS サーバー・プロパティーの編集

ネーム・サーバー作成後、allow-update やデバッグのレベルなどのプロパティーを編集することができます。これらのオプションは、変更するサーバー・インスタンスにのみ適用されます。

DNS サーバー・インスタンスのプロパティーを編集するには、以下のステップに従ってください。

1. 「**iSeries ナビゲーター**」で、「**使用する iSeries サーバー**」 → 「**ネットワーク**」 → 「**サーバー**」 → 「**DNS**」と展開します。

2. 右側のペインで、「**使用する DNS サーバー**」を右クリックし、「**構成**」を選択します。
3. 「**DNS サーバー**」を右クリックし、「**プロパティー**」を選択します。

ネーム・サーバー上のゾーンの構成

DNS サーバー・インスタンスを構成したら、次に、ネーム・サーバーのゾーンを構成する必要があります。

ご使用のサーバーは右側のペインに表示されます。ご使用のサーバー上にゾーンを構成するには、サーバー名を右クリックし、「**構成**」を選択します。「DNS 構成」ウィンドウが表示されます。

すべてのゾーンはウィザードを使用して構成されます。関連するフォルダーを右クリックし、「**前方参照ゾーン**」または「**逆引き参照ゾーン**」を作成します。そのゾーン・タイプ用のオプションが表示されます。作成したいゾーン・タイプを選択して、ウィザードを開始します。

関連概念

30 ページの『外部 DNS データのアクセス』
DNS ゾーン・データを作成すると、ご使用のサーバーはそのゾーンに対する照会に回答できます。

関連タスク

『動的更新を受信するための DNS の構成』
BIND 8 で実行される DNS サーバーは、 ゾーン・データを動的に更新する他ソースからの要求を受け入れるように構成することができます。 このトピックでは、allow-update オプションの構成手順を説明します。 それにより、DNS が動的更新を受信できるようになります。

29 ページの『DNS ファイルのインポート』
DNS は既存のゾーン・データ・ファイルをインポートすることができます。 既存構成ファイルから新しいゾーンを作成するために、上記の時間のかからない手順に従ってください。

関連資料

2 ページの『ゾーンについて』
このトピックでは、ドメイン・ネーム・システム (DNS) のゾーンおよびゾーンのタイプについて説明します。

動的更新を受信するための DNS の構成

BIND 8 で実行される DNS サーバーは、ゾーン・データを動的に更新する他ソースからの要求を受け入れるように構成することができます。このトピックでは、allow-update オプションの構成手順を説明します。それにより、DNS が動的更新を受信できるようになります。

動的ゾーン作成時、ネットワーク構造を考慮する必要があります。ドメインの一部がまだ手動による更新を必要とする場合、静的ゾーンと動的ゾーンを別個にセットアップする必要があります。動的ゾーンに対して手動による更新を行う場合、動的ゾーンのサーバーを停止して、更新完了後に再始動する必要があります。サーバーを停止することは、サーバーがゾーン・データベースからゾーン・データをロードした時点以降に行った、すべての動的更新を強制的に同期化することを意味します。サーバーを停止しない場合、サーバーが最後に開始してから処理されたすべての動的更新は失われます。ただし、サーバーを停止して手動による更新を行う場合、サーバーが停止中に送信された動的更新は失われることになります。

オブジェクトが allow-update ステートメントで定義されていると、DNS はゾーンが動的であることを示します。 allow-update オプションを構成するには、以下のステップに従ってください。

1. iSeries ナビゲーターで、「**使用する iSeries サーバー** 」 → 「**ネットワーク**」 → 「**サーバー**」 → 「**DNS**」と展開します。
2. 右側のペインで、「**使用する DNS サーバー**」を右クリックし、「**構成**」を選択します。

3. 「DNS 構成」ウィンドウで、「**前方参照ゾーン**」または「**逆引き参照ゾーン**」を展開します。
4. 編集したい 1 次ゾーンを右クリックして「**プロパティー**」を選択します。
5. 「1 次ゾーン・プロパティー」ページで「**オプション**」タブをクリックします。
6. 「オプション」ページで、「**アクセス制御**」 → 「**allow-update**」と展開します。
7. DNS はアドレス・マッチ・リストを使用して、許可された更新を検証します。アドレス・マッチ・リストにオブジェクトを追加するには、アドレス・マッチ・リストの要素タイプを選択し「**追加**」をクリックします。 IP アドレス、IP 接頭部、アクセス制御リスト、またはキーを追加できます。
8. アドレス・マッチ・リストの更新が終了したら、「**OK**」をクリックして、「オプション」ページを閉じます。

関連概念

5 ページの『動的更新』
OS/400 V5R1 DNS (BIND 8 ベース) は、動的更新をサポートします。これにより、DHCP などの外部ソースが DNS サーバーに更新を送信できるようになります。

28 ページの『ネーム・サーバー上のゾーンの構成』
DNS サーバー・インスタンスを構成したら、 次に、ネーム・サーバーのゾーンを構成する必要があります。

関連タスク

動的更新を送信する DHCP 構成

DNS ファイルのインポート

DNS は既存のゾーン・データ・ファイルをインポートすることができます。既存構成ファイルから新しいゾーンを作成するために、上記の時間のかからない手順に従ってください。

ゾーン・データ・ファイルをインポートするか、または既存のホスト・テーブルを変換することによって 1 次ゾーンを作成することができます。ホスト・テーブルからゾーン・データを作成するには、『ホスト・テーブルの変換』を参照してください。

BIND 構文に基づく有効なゾーン構成ファイルであれば、任意のファイルをインポートできます。このファイルは IFS ディレクトリーに配置する必要があります。インポートされると、DNS はそれが有効なゾーン・データ・ファイルであることを確認し、このサーバー・インスタンスの NAMED.CONF ファイルに追加します。

ゾーン・ファイルをインポートするには、以下のステップに従ってください。

1. iSeries ナビゲーターで、「**使用する iSeries サーバー** 」 → 「**ネットワーク**」 → 「**サーバー**」 → 「**DNS**」と展開します。
2. 右側のペインで、ゾーンをインポートしたい DNS サーバー・インスタンスをダブルクリックします。
3. 左側のペインで「**DNS サーバー**」を右クリックし、「**ゾーンのインポート**」を選択します。
4. ウィザードの指示に従って、1 次ゾーンをインポートします。

関連概念

28 ページの『ネーム・サーバー上のゾーンの構成』
DNS サーバー・インスタンスを構成したら、 次に、ネーム・サーバーのゾーンを構成する必要があります。

レコードの妥当性検査

ドメイン・データ・インポート機能は、インポート予定のファイルの各レコードを読み込んで妥当性検査します。

ドメイン・データ・インポート機能が完了すると、エラーとなったすべてのレコードが、インポートされたゾーンの「別のレコード」プロパティー・ページ上で個々に調べられます。

注:

1. 大規模な 1 次ドメインをインポートすると、数分かかる場合があります。
2. ドメイン・データ・インポート機能は $include ディレクティブをサポートしません。ドメイン・データ・インポート機能の妥当性検査プロセスは、$include ディレクティブを含んだ行をエラーのある行として識別します。

外部 DNS データのアクセス

DNS ゾーン・データを作成すると、ご使用のサーバーはそのゾーンに対する照会に回答できます。

ルート・サーバーは、インターネットまたは大規模イントラネットに直接接続している DNS サーバーの機能にとって非常に重要です。DNS サーバーは、ルート・サーバーを使用して、自分のドメイン・ファイル中に入っているホスト以外のホストに関する照会に応答する必要があります。

詳しい情報を得るためには、DNS サーバーはどこを探せばよいかを知っている必要があります。インターネット上で、DNS サーバーが最初に探す場所がルート・サーバーです。 ルート・サーバーは、照会への応答が見付かるか応答できないと分かるまで、DNS サーバーに階層の他のサーバーへの経路を指示します。

iSeries ナビゲーターのデフォルト・ルート・サーバー・リスト

インターネット・ルート・サーバーは、インターネット接続があり、かつ自分の DNS サーバーでは解決できない時にインターネット上で名前を解決したい場合に限って、使用してください。インターネット・ルート・サーバーのデフォルト・リストは、 iSeries ナビゲーターにあります。そのリストは、iSeries ナビゲーターがリリースされた時点のものです。このデフォルト・リストを InterNIC サイト上のリストと比較して、デフォルト・リストが最新版であるかを確認することができます。ご使用の構成のルート・サーバー・リストが常に最新状態になるように更新してください。

インターネットのルート・サーバー・アドレスの入手先

階層の最上位にあるルート・サーバーのアドレスは時々刻々変化します。これを最新状態に保つ責任は、DNS の管理者にあります。 InterNIC はインターネットのルート・サーバー・アドレスの最新リストを維持管理します。インターネットのルート・サーバー・アドレスの最新リストを入手するには、以下の手順に従ってください。

1. InterNIC サーバー: `FTP.RS.INTERNIC.NET` に匿名 FTP を行います。
2. ファイル: `/domain/named.root` をダウンロードします。
3. そのファイルをディレクトリー・パス: `Integrated File System/Root/QIBM/ProdData/OS400/DNS/ROOT.FILE` に格納します。

ファイアウォールの後ろ側にある DNS には、ルート・サーバーが定義されていない場合があります。この場合、DNS サーバーは、それ自身の 1 次ドメイン・データベース・ファイルまたはキャッシュに存在するエントリーからのみ、照会を解決することができます。このサーバーはオフサイト照会をファイアウォール DNS に転送する場合があります。この場合、ファイアウォール DNS サーバーは転送者のように機能します。

イントラネット・ルート・サーバー

ご使用の DNS サーバーが大規模イントラネットの一部の場合、内部ルート・サーバーを持つ場合があります。ご使用の DNS サーバーがインターネットにアクセスしない場合は、デフォルトのインターネット・サーバーをロードする必要はありません。ただし、ご使用の DNS サーバーがそのドメイン外の内部アドレスを解決できるように、内部ルート・サーバーを追加する必要があります。

関連概念

28 ページの『ネーム・サーバー上のゾーンの構成』
DNS サーバー・インスタンスを構成したら、 次に、ネーム・サーバーのゾーンを構成する必要があります。

DNS の管理

このトピックでは、DNS 機能の検証方法、パフォーマンスのモニター方法、および DNS データとファイルの管理方法について説明します。

ネーム・サーバー・ルックアップによる DNS の検証

ネーム・サーバー・ルックアップ (NSLookup) を使用して、DNS が作動していることを検査できます。

DNS サーバーを IP アドレスで照会するために、NSLookup (ネーム・サーバー検索) を使用します。これにより、DNS が照会に応答できるかどうかを検証します。ループバック IP アドレス (127.0.0.1) に関連したホスト名を要求します。ホスト名 (localhost) で応答される必要があります。検証しようとするサーバー・インスタンスに定義された特定の名前も照会する必要があります。これにより、テストしている特定サーバー・インスタンスが正しく機能していることを確認できます。

NSLookup で DNS 機能を検証するには、以下のステップに従ってください。

1. コマンド行で「NSLOOKUP DMNNAMSVR(n.n.n.n)」と入力します。ここで、n.n.n.n は、テストで listen する構成済みのサーバー・インスタンスのアドレスです。
2. コマンド行で 「NSLOOKUP」と入力し、「Enter」を押します。 これにより、NSLookup 照会セッションが開始します。
3. ご使用のサーバー名の前に「server」と入力して、「Enter」を押します。たとえば、「server myiseries.mycompany.com」のように入力します。この結果、以下のように表示されます。

   ```
   Server:  myiseries.mycompany.com
   Address: n.n.n.n
   ```

   ここで、n.n.n.n は、ご使用の DNS サーバーの IP アドレスを意味します。
4. コマンド行で「127.0.0.1」と入力し、「Enter」を押します。

   この結果、ループバック・ホスト名を含んで、以下の情報が表示されます。

   ```
    > 127.0.0.1
   サーバー:  myiseries.mycompany.com
   アドレス:  n.n.n.n


   名前:    localhost
     Address:  127.0.0.1
   ```

   DNS サーバーがループバック・ホスト名「**localhost**」を戻した場合は、その DNS サーバーは正しく応答しています。
5. 「exit」と入力し、「Enter」を押して NSLOOKUP 端末セッションを終了します。

注: NSLookup 使用上でヘルプが必要な場合は ? と入力してください。そして「Enter」を押します。

セキュリティー・キーの管理

セキュリティー・キーにより、ご使用の DNS データへのアクセスを制限できるようになります。

DNS に関連する 2 つのタイプのキーがあります。この各キーはご使用の DNS 構成を保護する上で異なる役割を果たします。以下に、各キーが DNS サーバーにどのように関連するかを説明します。

DNS キーの管理

DNS キーは、BIND のために定義され、送られてくる更新の検証処理の一環として DNS サーバーによって使用されるキーです。

キーを構成し、それに名前を付けることができます。それから、DNS オブジェクト (動的ゾーンなど) を保護したい場合、アドレス・マッチ・リスト中にキーを指定できます。

DNS キーを管理するには、以下のステップに従ってください。

1. iSeries ナビゲーターで、「**使用する iSeries サーバー** 」 → 「**ネットワーク**」 → 「**サーバー**」 → 「**DNS**」と展開します。
2. 右側のペインで、オープンしたい DNS サーバー・インスタンスを右クリックし、「**構成**」を選択します。
3. 「DNS 構成」ウィンドウで、「**ファイル**」 → 「**キーの管理**」と選択します。

動的更新キーの管理

動的更新キーは、DHCP による動的更新を保護するのに使用します。

これらのキーは、DNS と DHCP が同じ iSeries 上にある場合に必要になります。 DHCP が別の iSeries にある場合は、各 iSeries サーバー上に同じ動的更新キーを作成して、動的更新の保護ができるようにする必要があります。

動的更新キーを管理するには、以下のステップに従ってください。

1. iSeries ナビゲーターで、「**使用する iSeries サーバー** 」 → 「**ネットワーク**」 → 「**サーバー**」 → 「**DNS**」と展開します。
2. 「**DNS**」を右クリックし、「**動的更新キーの管理**」を選択します。

DNS サーバー統計の使用

データベース・ダンプおよび統計ツールは、サーバーのパフォーマンスを検討および管理するのに有効です。

DNS には、いくつかの診断ツールがあります。サーバーのパフォーマンスをモニターするのに使用できます。

関連資料

33 ページの『DNS 構成ファイルの維持管理』
このトピックでは、DNS が使用するファイルについて理解していただくためと、 そのファイルをバックアップし維持管理するためのガイドラインを検討していただくための概要を説明します。

サーバー統計

サーバー統計は、サーバーの最後の再始動またはデータベースの再ロード以降に、そのサーバーが受信した照会と応答の数を要約したものです。

DNS では、サーバー・インスタンスの統計を表示することができます。統計情報は継続的にこのファイルに追加され、このファイルが削除されるまで続きます。この情報は、サーバーが受信しているトラフィックの量の評価、および、問題のトラッキングに役立ちます。サーバー統計についての詳細は、DNS のオンライン・ヘルプ・トピックの「DNS サーバー統計について」で入手可能です。

サーバー統計にアクセスするには、以下のステップに従ってください。

1. iSeries ナビゲーターで、「**使用する iSeries サーバー** 」 → 「**ネットワーク**」 → 「**サーバー**」 → 「**DNS**」と展開します。
2. 右側のペインで、「**使用する DNS サーバー**」を右クリックし、「**構成**」を選択します。
3. 「DNS 構成」ウィンドウで、「**表示**」 → 「**サーバー統計**」を選択します。

アクティブ・サーバー・データベース

アクティブ・サーバー・データベースには、ゾーンとホスト情報が含まれています。この情報には、一部のゾーン・プロパティー (権限付与の開始 (SOA) 情報など)、および全ホスト・プロパティー (メール・エクスチェンジャー (MX) 情報など) が含まれており、問題をトラッキングするのに役立ちます。

DNS により、許可データ、キャッシュ・データ、およびサーバー・インスタンスに対する障害判別のヒントとなるデータのダンプを表示できるようになります。 このダンプには、サーバーが照会から入手した情報と、すべてのサーバーの 1 次および 2 次ゾーン (順および逆マッピング・ゾーン) からの情報が含まれています。

iSeries ナビゲーターを使用して、アクティブ・サーバー・データベースのダンプを表示できます。このファイルのコピーを保管する必要がある場合、そのデータベース・ダンプ・ファイルの名前は、NAMED_DUMP.DB であり、 iSeries ディレクトリー・パス (**Integrated File System/Root/QIBM/UserData/OS400/DNS/<server instance>**) にあります。ここで、″<server instance>″ は DNS サーバー・インスタンスの名前です。アクティブ・サーバー・データベースの詳細は、DNS のオンライン・ヘルプ・トピックの「**DNS サーバー・データベース・ダンプについて**」で入手可能です。

アクティブ・サーバー・データベース・ダンプにアクセスするには、以下のステップに従ってください。

1. iSeries ナビゲーターで、「**使用する iSeries サーバー** 」 → 「**ネットワーク**」 → 「**サーバー**」 → 「**DNS**」と展開します。
2. 右側のペインで、「**使用する DNS サーバー**」を右クリックし、「**構成**」を選択します。
3. 「DNS 構成」ウィンドウで、「**表示**」 → 「**アクティブ・サーバー・データベース**」を選択します。

DNS 構成ファイルの維持管理

このトピックでは、DNS が使用するファイルについて理解していただくためと、そのファイルをバックアップし維持管理するためのガイドラインを検討していただくための概要を説明します。

i5/OS DNS を使用して、 iSeries 上で、DNS サーバー・インスタンスを作成し管理できます。 DNS の構成ファイルは、iSeries ナビゲーターによって管理されます。このファイルは、手動で編集しないでください。 DNS 構成ファイルの作成、変更、および削除は、必ず、iSeries ナビゲーターを使用して行ってください。 DNS 構成ファイルは、以下にリストされた統合ファイル・システムのパスに保管されます。

注: 以下のファイル構造は、BIND 8 で実行される DNS に適用されます。 BIND 4.9.3 ベースの DNS をご使用の場合は、V4R5 DNS Information Center トピックの「DNS 構成ファイルのバックアップとログ・ファイルの維持管理」を参照してください。

以下の表には、各ファイルがパスの階層順にリストされています。保管アイコン  が付いているファイルは、データを保護するためにバックアップをとってください。削除アイコン  が付いているファイルは、定期的に削除してください。

名前	アイコン	説明
QIBM/UserData/OS400/DNS/		DNS 用の開始点ディレクトリー。
ATTRIBUTES		DNS はこのファイルを使用して、どのバージョンの BIND を使用しているかを判別します。
QIBM/UserData/OS400/DNS/ ***<instance-n>/***		DNS インスタンス用の開始点ディレクトリー。
ATTRIBUTES		iSeries DNS によって使用される構成属性。
NAMED.CONF		このファイルには構成データが含まれます。管理する特定ゾーン、ゾーン・ファイルの場所、動的に更新されるゾーン、転送先サーバーの場所、およびその他のオプション設定をサーバーに知らせるのに使用されます。
BOOT.AS400BIND4		BIND 4.9.3 サーバー構成およびポリシー・ファイル。このファイルはこのインスタンス用の BIND 8 NAMED.CONF ファイルへ変換されます。このファイルは、BIND 4.9.3 サーバーを BIND 8 にマイグレーションする場合に作成されます。このファイルは、マイグレーション用のバックアップとして機能し、BIND 8 が正常に作動すれば削除しても構いません。
NAMED.CA		このサーバー・インスタンス用のルート・サーバー・リスト。
NAMED_DUMP.DB		アクティブ・サーバー・データベース用に作成されたサーバー・データ・ダンプ。
NAMED.STATS		サーバー統計。
NAMED.PID		実行中サーバーの Process ID を保持。このファイルは、DNS サーバーが始動するたびに、作成されます。このファイルは、データベース、統計、および更新サーバー用に使用されます。このファイルは編集または削除しないでください。

名前	アイコン	説明
QUERYLOG		受信した照会の DNS サーバー・ログ。このファイルは、DNS サーバー・ログがアクティブになると、作成されます。アクティブ時は、このファイルは大きくなるため、定期的に削除する必要があります。
<*zone-name-a*>.DB		このサーバーが提供する特定ドメイン用のゾーン・ファイル。このゾーン用のリソース・レコードすべてが含まれます。
<*zone-name-b*>.DB		このサーバーが提供する特定ドメイン用のゾーン・ファイル。このゾーン用のリソース・レコードすべてが含まれます。各ゾーンには個別の .DB ファイルがあります。
.ixfr.		増分ゾーン転送 (IXFR) ファイル。このファイルは 2 次サーバーが使用して、最後のゾーン転送以降に発生した変分データのみロードします。更新が行われると、IXFR ファイルの数が増加します。古い IXFR ファイルは定期的に削除してください。過去 1 から 2 日内に作成されたファイルを残しておくと、ほとんどの 2 次サーバーが引き続き IXFR をロードできます。このファイルのすべてを削除すると、2 次サーバーは完全転送 (AXFR) を要求します。
TMP		一時的作業ファイルの作成用に、サーバー・インスタンスが使用するディレクトリー。
QIBM/UserData/OS400/DNS/TMP		QTOBH2N プログラムが使用する一時的なディレクトリー。 QTOBH2N プログラムは、iSeries ナビゲーターを使用して後でインポートするために、ホスト・テーブルからダンプされた中間ファイルを作成します。
QIBM/UserData/OS400/DNS/_DYN/		動的更新に必要なファイルを保持するディレクトリー。
<*key_id-name-x*>._KID		<*key_id-name-x*> という名の key_id で、BIND 8 キー・ステートメントを含むファイル。
<*key_id-name-x*>._DUK. <*zone-name-a*>		<*key_id-name-x*> キーを使用して、<*zone-name-a*> への動的更新要求を開始するのに必要な動的更新キー。
<*key_id-name-y*>._KID		<*key_id-name-y*> という名の key_id で、BIND 8 キー・ステートメントを含むファイル。

名前	アイコン	説明
<*key_id-name-y*>._DUK. <*zone-name-a*>		<*key_id-name-y*> キーを使用して、 <*zone-name-a*> への動的更新要求を開始するのに必要な動的更新キー。
<*key_id-name-y*>._DUK. <*zone-name-b*>		<*key_id-name-y*> キーを使用して、 <*zone-name-b*> への動的更新要求を開始するのに必要な動的更新キー。

関連概念

22 ページの『DNS 権限の決定』
DNS 管理者に対して特別な許可要件があります。 許可が意味するセキュリティーについても検討する必要があります。

32 ページの『DNS サーバー統計の使用』
データベース・ダンプおよび統計ツールは、サーバーのパフォーマンスを検討および管理するのに有効です。

関連タスク

26 ページの『ネーム・サーバーの構成』
DNS を使用すると、複数のネーム・サーバー・インスタンスを作成できます。このトピックではネーム・サーバーの構成手順を説明します。

拡張 DNS 機能

このトピックでは、経験のある管理者が、DNS の拡張機能を使用して、 DNS サーバーをもっと簡単に管理する方法について説明します。

iSeries ナビゲーターの中で DNS は、DNS サーバーを構成および管理するためのインターフェースを提供します。以下のタスクがショートカットとして、iSeries グラフィカル・インターフェースに精通した管理者に提供されます。 このインターフェースは、複数インスタンスのサーバー状況および属性を一度に変更するための、迅速な方法を提供します。

関連タスク

40 ページの『DNS デバッグ設定値の変更』
DNS のデバッグ機能は、DNS サーバーの問題を判別し修正するのに役立つ情報を提供します。

DNS 属性の変更

DNS インターフェースが、すべてのサーバー・インスタンスの自動開始とデバッグ・レベルを一度に変更することを許可しない場合でも、DNS 設定値を変更できます。

文字ベースのインターフェースを使用して個別に DNS サーバー・インスタンスに対してこれらの設定を変更するか、または一度にすべてのインスタンスに対して変更することができます。CHGDNSA を使用する以下のステップに従ってください。

1. コマンド行で、「CHGDNSA」と入力して「F4」を押します。
2. 「DNS サーバー属性の変更 (CHGDNSA)」ページで、単一サーバー・インスタンスの名前を入力するか「*ALL」 と入力して、「Enter」を押します。

   以下の、使用可能なサーバー属性オプションが表示されます。

```
Autostart server . . . . . *SAME *YES, *NO, *SAME
Debug level . . . . . *SAME 0-11, *SAME, *DFT
```

3. **自動開始** 選択された DNS サーバーが TCP/IP 始動時に自動開始するように指定するには、 「*YES」と入力してください。 TCP/IP 始動時にサーバーが開始しないようにするには、「*NO」と入力してください。現行の設定のままで属性を残したい場合は「*SAME」と入力してください。

   デバッグ・レベル 選択された DNS サーバーが使用するデバッグ・レベルを変更するには、0 から 11 の値を入力します。サーバー始動時のデバッグ・レベルを継承して使用したい場合は「*DFT」と入力します。現行の設定のままで属性を残したい場合は「*SAME」と入力してください。

   すべてのプリファレンスを入力完了後は「Enter」を押して、DNS 属性を設定します。

DNS サーバーの始動または停止

DNS インターフェースが複数のサーバー・インスタンスを一度に始動または停止することを許可しない場合、設定値を変更することができます。

文字ベースのインターフェースを使用して複数インスタンスに対するこの設定を一度に変更することができます。文字ベースのインターフェースを使用してすべての DNS サーバー・インスタンスを一度に始動するには、コマンド行で STRTCPSVR SERVER(*DNS) DNSSVR(*ALL) と入力してください。すべての DNS サーバーを一度に停止するには、コマンド行で ENDTCPSVR SERVER(*DNS) DNSSVR(*ALL) と入力してください。

デバッグ値の変更

デバッグ・レベルを変更することができます。この機能は、大規模ゾーンを持ち、大量のデバッグ・データ (サーバーが最初に始動して、そのゾーン・データすべてをロードしている間に入手されるデータ) が不要な管理者にとって便利です。

iSeries ナビゲーター・インターフェースで、DNS は、稼働中サーバーのデバッグ・レベルを変更することを許可しません。 ただし、文字ベースのインターフェースを使用して、稼働中サーバーのデバッグ・レベルを変更できます。文字ベースのインターフェースを使用してデバッグ・レベルを変更するには、以下のステップに従って、<instance> をサーバー・インスタンス名で置き換えてください。

1. コマンド行で「ADDLIBLE QDNS」と入力して「Enter」を押します。
2. デバッグ・レベルを以下のようにして変更します。
   - デバッグをオンにするか、またはデバッグ・レベルを 1 ずつ増やすには、 「CALL QTOBDRVS ('BUMP' '<instance>')」と入力して「Enter」を押します。
   - デバッグをオフにするには、 「CALL QTOBDRVS ('OFF' '<instance>')」と入力して「Enter」を押します。

DNS のトラブルシューティング

このトピックでは、DNS サーバーで発生した問題を解決するのに有効な、DNS ロギングおよびデバッグ設定値について説明します。

DNS は、他の TCP/IP 機能およびアプリケーションとほぼ同じように機能します。 DNS ジョブは、SMTP または FTP アプリケーションと同じように、QSYSWRK サブシステムのもとで実行され、それによって、この DNS ジョブに関連した情報を含むジョブ・ログを、ユーザー・プロファイル QTCP の下に作成します。DNS ジョブが終了すると、原因を判別するためにそのジョブ・ログを使用できます。 DNS サーバーが期待していた応答を戻さない場合、問題分析に役立つ情報がジョブ・ログに含まれていることがあります。

DNS 構成は、異なるタイプのレコードが入っている複数のファイルによって構成されます。DNS サーバーの問題は、一般には DNS 構成ファイルのエントリーが誤っていることが原因です。問題が生じたときには、DNS 構成ファイルに、期待した項目が入っているか確認してください。

ジョブの識別

ジョブ・ログの中を探して DNS サーバー機能 (たとえば、WRKACTJOB の使用) を検証したい場合、以下に示すネーミング・ガイドラインを検討してください。

- BIND 4.9.3 を使用している場合、サーバーのジョブ名は QTOBDNS となります。 DNS 4.9.3 のデバッグについて詳しくは、「*Troubleshooting DNS servers (DNS* サーバーのトラブルシューティング)」を参照してください。
- BIND 8 ベースのサーバーを稼働している場合、稼働しているサーバー・インスタンスごとに個別のジョブがあります。ジョブ名は 5 文字 (QTOBD) 固定で、インスタンス名が続きます。たとえば、INST1 と INST2 という 2 つのインスタンスがある場合、そのジョブ名は QTOBDINST1 と QTOBDINST2 になります。

関連概念

『DNS サーバー・メッセージのロギング』
DNS には多くのロギング・オプションがあり、ユーザーはこれらのオプションを調整して、 問題の原因の検出にあたることができます。 ロギングには、各種の重大度レベル、メッセージ・カテゴリー、および出力ファイルを提供することにより、柔軟性があります。 それにより、ロギングを正しくチューニングして問題発見に役立てることができます。

関連タスク

40 ページの『DNS デバッグ設定値の変更』
DNS のデバッグ機能は、DNS サーバーの問題を判別し修正するのに役立つ情報を提供します。

DNS サーバー・メッセージのロギング

DNS には多くのロギング・オプションがあり、ユーザーはこれらのオプションを調整して、問題の原因の検出にあたることができます。ロギングには、各種の重大度レベル、メッセージ・カテゴリー、および出力ファイルを提供することにより、柔軟性があります。それにより、ロギングを正しくチューニングして問題発見に役立てることができます。

BIND 8 はいくつかの新しいロギング・オプションを提供します。ログに記録するメッセージ・タイプ、各メッセージ・タイプの送信先、およびログに記録する各メッセージ・タイプの重大度を指定できます。一般的に、デフォルトのロギング設定値は適切と考えられますが、設定を変更する場合は、ロギングについて、BIND 8 に関するその他の情報を参照することをお勧めします。

ロギング・チャネル

DNS サーバーはさまざまな出力チャネルに、メッセージを記録することができます。チャネルはログ・データの送信先を指定します。以下のチャネル・タイプを選択できます。

- **ファイル・チャネル**

  ファイル・チャネルにログ記録されるメッセージはファイルに送信されます。デフォルトのファイル・チャネルは、as400_debug と as400_QPRINT です。デフォルトにより、デバッグ・メッセージは as400_debug チャネルにログ記録されます。これは NAMED.RUN ファイルです。しかし、他のメッセージ・カテゴリーも同様にこのファイルに送信することができます。 as400_QPRINT にログ記録されるメッセージ・カテゴリーは、ユーザー・プロファイル QTCP 用の QPRINT スプール・ファイルに送信されます。提供されたデフォルトのチャネルの他に、自分自身のファイル・チャネルを作成できます。

- **SYSLOG チャネル**

  このチャネルにログ出力されたメッセージは、サーバーのジョブ・ログに送信されます。デフォルトの syslog チャネルは as400_joblog です。このチャネルにルーティングされたロギング・メッセージは、DNS サーバー・インスタンスのジョブ・ログに送信されます。
- **ヌル・チャネル**

  ヌル・チャネルにログ記録された全メッセージは廃棄されます。デフォルトのヌル・チャネルは as400_null です。どのログ・ファイルにもメッセージを出力したくない場合、ヌル・チャネルにカテゴリーをルーティングすることができます。

メッセージ・カテゴリー

メッセージはカテゴリーにグループ化されます。各チャネルにログ記録されるメッセージ・カテゴリーを指定することができます。以下のような、多くのカテゴリーがあります。

- config: 構成ファイル処理
- db: データベース操作
- queries: サーバーが受信する各照会ごとに短いログ・メッセージを生成
- lame-servers: 間違った照会代行の検出
- update: 動的更新
- xfer-in: サーバーが受信しているゾーン転送
- xfer-out: サーバーが送信しているゾーン転送

ログ・ファイルは大きくなるため、定期的に削除する必要があります。すべての DNS サーバーのログ・ファイルは、DNS サーバーを停止して始動するとクリアされます。

メッセージ重大度

チャネルは、メッセージ重大度によりメッセージをフィルターに掛けることができます。各チャネルごとに、メッセージがログ出力される重大度レベルを指定することができます。以下に、使用可能な重大度レベルを示します。

- 重大
- エラー
- 警告
- 注意
- 通知
- デバッグ (デバッグ・レベル 0 から 11 を指定)
- 動的 (サーバー始動時のデバッグ・レベルを継承)

上記リスト中で選択した重大度および指定したレベルより高い重大度レベルを持つすべてのメッセージがログに記録されます。たとえば、警告を選択した場合、チャネルは警告、エラー、および重大メッセージをログに記録します。デバッグ・レベルを選択した場合、デバッグ・メッセージをログ出力したい 0 から 11 の値を指定できます。

ログ設定の変更

ロギング・オプションにアクセスするには、以下のステップに従ってください。

1. iSeries ナビゲーターで、**「使用する iSeries サーバー 」 → 「ネットワーク」 → 「サーバー」 → 「DNS」**と展開します。
2. 右側のペインで、**「使用する DNS サーバー」**を右クリックし、**「構成」**を選択します。
3. 「DNS 構成」ウィンドウで**「DNS サーバー」**を右クリックし、**「プロパティー」**を選択します。
4. 「サーバー・プロパティー」ウィンドウで**「チャネル」**タブを選択します。これは、新規のファイル・チャネルまたはチャネルのプロパティー (各チャネルにログ記録されるメッセージ重大度など) を作成するためです。
5. 「サーバー・プロパティー」ウィンドウで、**「ロギング」**タブを選択します。これは、どのメッセージ・カテゴリーが各チャネルにログ出力されるかを指定するためです。

トラブルシューティングのヒント

as400_joblog チャネルのデフォルト重大度レベルは、エラーに設定されています。この設定は、通知レベルおよび警告レベルのメッセージの量を減少させるために使用されます。そうしないと、パフォーマンスの低下を起こす可能性があります。問題が発生して、その問題の原因がジョブ・ログに示されていない場合、重大度レベルを変更する必要があります。上記の手順に従って「チャネル」ページにアクセスし、as400_joblog チャネルの重大度レベルを、警告、注意、または通知のいずれかに変更してください。そうすれば、より多くのログ・データを表示することができます。問題が解決した後は、重大度レベルをエラーに戻してジョブ・ログに出力されるメッセージ数を減少させます。

関連タスク

37 ページの『DNS のトラブルシューティング』
このトピックでは、DNS サーバーで発生した問題を解決するのに有効な、DNS ロギングおよびデバッグ設定値について説明します。

DNS デバッグ設定値の変更

DNS のデバッグ機能は、DNS サーバーの問題を判別し修正するのに役立つ情報を提供します。

DNS は 12 レベルでデバッグをコントロールします。ロギングは、通常、容易に問題を発見する方法を提供しますが、ある場合には、デバッグすることが必要になります。通常の状態では、デバッグはオフ (値を 0 にする) にします。 まず最初にロギングを使用して問題修正を試みることをお勧めします。

有効なデバッグ・レベルは、0 から 11 です。 IBM サービス技術員は、DNS の問題を診断するのに適切なデバッグ値を決定するためのサポートを行うことができます。 1 またはそれ以上の値は、デバッグ情報を iSeries ディレクトリー・パス (**Integrated File System/Root/QIBM/UserData/OS400/DNS/<server instance>**) にある NAMED.RUN ファイルに出力します。ここで、″<server instance>″ は DNS サーバー・インスタンスの名前です。 NAMED.RUN ファイルは、デバッグ・レベルが 1 またはそれ以上に設定されて DNS が実行され続ける限り、増え続けます。あまり多くのディスク・スペースを使用しないように、時々、そのファイルを削除することをお勧めします。また、**「サーバー・プロパティー - チャネル」**ページを使用して、NAMED.RUN ファイルの最大サイズとバージョン数のプリファレンスを指定することができます。

DNS サーバー・インスタンスのデバッグ値を変更するには、以下のステップに従ってください。

1. iSeries ナビゲーターで、**「使用する iSeries サーバー 」 → 「ネットワーク」 → 「サーバー」 → 「DNS」**と展開します。
2. 右側のペインで、**「使用する DNS サーバー」**を右クリックし、**「構成」**を選択します。
3. 「DNS 構成」ウィンドウで、「DNS サーバー」を右クリックし、**「プロパティー」**を選択します。
4. 「サーバー・プロパティー - 一般」ページで、サーバー始動時のデバッグ・レベルを指定します。

5. サーバーが稼働中の場合は、サーバーをいったん停止して再始動してください。

注: デバッグ・レベルを変更しても、サーバーの稼働中はその変更が有効になりません。ここで設定されたデバッグ・レベルはそのサーバーが次回、完全再始動される時に有効になります。サーバーが稼働中にデバッグ・レベルを変更する必要がある場合は、『拡張 DNS 機能』を参照してください。

関連概念

36 ページの『拡張 DNS 機能』
このトピックでは、 経験のある管理者が、DNS の拡張機能を使用して、 DNS サーバーをもっと簡単に管理する方法について説明します。

関連タスク

37 ページの『DNS のトラブルシューティング』
このトピックでは、DNS サーバーで発生した問題を解決するのに有効な、DNS ロギングおよびデバッグ設定値について説明します。

DNS の関連資料

以下には、DNS トピックに関連した IBM Redbooks™ (PDF フォーマット) および Web サイトがリストされています。 PDF 資料は、いずれも、表示または印刷できます。

IBM Redbooks

AS/400® TCP/IP Autoconfiguration: DNS and DHCP Support 

この Redbook には、i5/OS に組み込まれている DNS サーバー・サポートおよび DHCP サーバー・サポートの説明が記載されています。このレッドブックの情報は、例を通して DNS および DHCP サポートのインストール、調整、構成、およびトラブルシューティングを行うのに役立ちます。

Web サイト

- *DNS and BIND* (第 3 版)。 Paul Albitz および Cricket Liu。 O'Reilly and Associates,Inc. 発行。  Sebastopol, California, 1998。 ISBN: 1-56592-512-2。これは DNS についての最も信頼のおける情報源です。
- Internet Software Consortium Web サイト  には、BIND に関するニュース、リンク、およびその他のリソースについての記載があります。
- InterNIC  サイトでは、Internet Corporation for Assigned Names and Numbers (ICANN) で許可されているすべてのドメイン・ネーム登録機関のディレクトリーを管理しています。
- DNS Resources Directory  には、DNS 参照資料、および、検討グループを含むその他の多くの DNS リソースへのリンクの記載があります。また、 DNS 関連 RFC  のリストの記載もあります。

PDF ファイルの保管

表示用または印刷用の PDF ファイルをワークステーションに保管するには、次のようにします。

1. ブラウザーで PDF ファイルを右マウス・ボタンでクリックする (上記のリンクを右マウス・ボタンでクリックする)。
2. PDF をローカルで保管するオプションをクリックする。
3. PDF ファイルを保管する先のディレクトリーを指定する。
4. 「**保管**」をクリックする。

Adobe Reader のダウンロード

これらの PDF を表示または印刷するには、システムに Adobe Reader がインストールされていることが必要です。Adobe Web サイト (www.adobe.com/products/acrobat/readstep.html)  から、無償コピーをダウンロードできます。

付録. 特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒106-0032
東京都港区六本木 3-2-31
IBM World Trade Asia Corporation
Licensing

以下の保証は、国または地域の法律に沿わない場合は、適用されません。 IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態で提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。 IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

IBM Corporation
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

本プログラムに関する上記の情報は、適切な使用条件の下で使用することができますが、有償の場合もあります。

© Copyright IBM Corp. 1998, 2006

本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定のプログラム契約の契約条項、IBM プログラムのご使用条件、IBM 機械コードのご使用条件、またはそれと同等の条項に基づいて、 IBM より提供されます。

この文書に含まれるいかなるパフォーマンス・データも、管理環境下で決定されたものです。そのため、他の操作環境で得られた結果は、異なる可能性があります。一部の測定が、開発レベルのシステムで行われた可能性がありますが、その測定値が、一般に利用可能なシステムのものと同じである保証はありません。さらに、一部の測定値が、推定値である可能性があります。実際の結果は、異なる可能性があります。お客様は、お客様の特定の環境に適したデータを確かめる必要があります。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。IBM は、それらの製品のテストは行っておりません。したがって、他社製品に関する実行性、互換性、またはその他の要求については確証できません。 IBM 以外の製品の性能に関する質問は、それらの製品の供給者にお願いします。

IBM の将来の方向または意向に関する記述については、予告なしに変更または撤回される場合があり、単に目標を示しているものです。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれています。より具体性を与えるために、それらの例には、個人、企業、ブランド、あるいは製品などの名前が含まれている場合があります。これらの名称はすべて架空のものであり、名称や住所が類似する企業が実在しているとしても、それは偶然にすぎません。

著作権使用許諾:

本書には、様々なオペレーティング・プラットフォームでのプログラミング手法を例示するサンプル・アプリケーション・プログラムがソース言語で掲載されています。お客様は、サンプル・プログラムが書かれているオペレーティング・プラットフォームのアプリケーション・プログラミング・インターフェースに準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。このサンプル・プログラムは、あらゆる条件下における完全なテストを経ていません。従って IBM は、これらのサンプル・プログラムについて信頼性、利便性もしくは機能性があることをほのめかしたり、保証することはできません。

それぞれの複製物、サンプル・プログラムのいかなる部分、またはすべての派生的創作物にも、次のように、著作権表示を入れていただく必要があります。

© (お客様の会社名) (西暦年). このコードの一部は、IBM Corp. のサンプル・プログラムから取られています。 © Copyright IBM Corp. _年を入れる_. All rights reserved.

この情報をソフトコピーでご覧になっている場合は、写真やカラーの図表は表示されない場合があります。

プログラミング・インターフェース情報

本書 (「DNS」) には、プログラムを作成するユーザーが IBM i5/OS のサービスを使用するためのプログラミング・インターフェースが記述されています。

商標

以下は、IBM Corporation の商標です。

| AFS
| AS/400
| e(ロゴ)server
| eServer
| i5/OS
| IBM
| IBM (ロゴ)
| iSeries
| OS/400
| Redbooks

他の会社名、製品名およびサービス名などはそれぞれ各社の商標または登録商標です。

使用条件

これらの資料は、以下の条件に同意していただける場合に限りご使用いただけます。

個人使用: これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、非商業的な個人による使用目的に限り複製することができます。ただし、IBM の明示的な承諾をえずに、これらの資料またはその一部について、二次的著作物を作成したり、配布 (頒布、送信を含む) または表示 (上映を含む) することはできません。

商業的使用: これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、お客様の企業内に限り、複製、配布、および表示することができます。ただし、IBM の明示的な承諾をえずにこれらの資料の二次的著作物を作成したり、お客様の企業外で資料またはその一部を複製、配布、または表示することはできません。

ここで明示的に許可されているもの以外に、資料や資料内に含まれる情報、データ、ソフトウェア、またはその他の知的所有権に対するいかなる許可、ライセンス、または権利を明示的にも黙示的にも付与するものではありません。

資料の使用が IBM の利益を損なうと判断された場合や、上記の条件が適切に守られていないと判断された場合、IBM はいつでも自らの判断により、ここで与えた許可を撤回できるものとさせていただきます。

お客様がこの情報をダウンロード、輸出、または再輸出する際には、米国のすべての輸出入関連法規を含む、すべての関連法規を遵守するものとします。

IBM は、これらの資料の内容についていかなる保証もしません。これらの資料は、特定物として現存するままの状態で提供され、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任なしで提供されます。

Printed in Japan

日本アイ・ビー・エム株式会社
〒106-8711　東京都港区六本木3-2-12