



System i

ネットワーキング

DNS (Domain Name System)

バージョン 6 リリース 1





System i

ネットワーキング

DNS (Domain Name System)

バージョン 6 リリース 1

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、49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 5761-SS1) バージョン 6 リリース 1 モディフィケーション 0 に適用されます。また、改訂版で断りが無い限り、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。

IBM 発行のマニュアルに関する情報のページ

<http://www.ibm.com/jp/manuals/>

こちらから、日本語版および英語版のオンライン・ライブラリーをご利用いただけます。また、マニュアルに関するご意見やご感想を、上記ページよりお送りください。今後の参考にさせていただきます。

(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： System i
Networking
Domain Name System
Version 6 Release 1

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 2008.2

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, 2008. All rights reserved.

© Copyright IBM Japan 2008

目次

DNS	1	ネーム・サーバー上のゾーンの構成	34
V6R1 の新機能	1	ネーム・サーバー上のビューの構成	34
ドメイン・ネーム・システムの PDF ファイル	3	動的更新を受信するためのドメイン・ネーム・システムの構成	35
ドメイン・ネーム・システムの概念	3	ドメイン・ネーム・システム・ファイルのインポート	35
ゾーンについて	4	レコードの妥当性検査	36
DNS 照会について	5	外部ドメイン・ネーム・システム・データへのアクセス	36
DNS ドメインのセットアップ	7	ドメイン・ネーム・システムの管理	37
動的更新	7	ドメイン・ネーム・システムが正しく機能しているかどうかの検証	37
BIND 9 の機能	9	セキュリティー・キーの管理	38
DNS リソース・レコード	11	ドメイン・ネーム・システム・キーの管理	38
メールおよびメール・エクスチェンジャー・レコード	16	動的更新キーの管理	38
例: ドメイン・ネーム・システム	17	ドメイン・ネーム・システム・サーバー統計の使用	39
例: イントラネット用単一 DNS サーバー	17	サーバー統計の使用	39
例: インターネット・アクセスを行う単一 DNS サーバー	19	アクティブ・サーバー・データベースへのアクセス	40
例: ドメイン・ネーム・システムと動的ホスト構成プロトコルが同一の System i 上にある場合	21	ドメイン・ネーム・システム構成ファイルの維持管理	40
例: 同一 System i 上に 2 つの DNS サーバーをセットアップしてファイアウォール上で DNS を分割する場合	23	拡張 DNS 機能	43
例: ビューを使用してファイアウォール上で DNS を分割する場合	26	ドメイン・ネーム・システム・サーバーの始動または停止	43
ドメイン・ネーム・システムの計画	28	デバッグ値の変更	43
ドメイン・ネーム・システム権限の決定	28	ドメイン・ネーム・システムのトラブルシューティング	44
ドメイン構造の決定	29	DNS サーバー・メッセージのロギング	44
セキュリティー基準の計画	30	ドメイン・ネーム・システムのデバッグ設定値の変更	47
DNS の要件	31	DNS の関連資料	48
ドメイン・ネーム・システムがインストールされているかどうかの判別	31	付録. 特記事項.	49
ドメイン・ネーム・システムのインストール	32	プログラミング・インターフェース情報	50
ドメイン・ネーム・システムの構成	32	商標	50
System i ナビゲーター でのドメイン・ネーム・システムへのアクセス	32	使用条件	51
ネーム・サーバーの構成	32		
ネーム・サーバー・インスタンスの作成	33		
ドメイン・ネーム・システム・サーバー・プロパティの編集	33		

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、ユーザーがホストを見つけるときに IP アドレス (IPv4 の場合は 192.168.12.88 など、IPv6 の場合は 2001:D88::1 など) ではなく、www.jkltoys.com のような単純名を使用することができます。1 つのサーバーは 1 つのゾーンのわずかな部分のホスト名と IP アドレスを知っているだけでよい場合がありますが、DNS サーバーは協同で働い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。DNS サーバーが協同して機能することにより、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なります。

IBM® i5/OS® バージョン 6 リリース 1 (V6R1) の場合、DNS サービスは Berkeley Internet Name Domain (BIND) バージョン 9 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 i5/OS リリースでは、DNS サービスは BIND バージョン 8.2.5 を基にしていました。新しい BIND バージョン 9 の DNS サーバーを使用するには、ご使用の IBM System i™ モデルに i5/OS オプション 31 (DNS) およびオプション 33 (ポータブル・アプリケーション・ソリューション環境 (PASE)) をインストールしておく必要があります。i5/OS V6R1 から、セキュリティ上の理由により BIND 4 および 8 は BIND 9 に置き換えられました。したがって、ご使用の DNS サーバーで BIND 9 へのマイグレーションを行う必要があります。

V6R1 の新機能

ドメイン・ネーム・システム (DNS) のトピック・コレクションに対して新規追加された情報や大幅に変更された情報について説明します。

BIND 9

今回のリリースで導入された Berkeley Internet Name Domain (BIND) バージョン 9 は、ドメイン・ネーム・システム (DNS) サーバーのパフォーマンスを向上するためにいくつかの機能を提供しています。例えば、バージョン 9 は IPv6 の現在定義されているすべての形式で、名前からアドレスおよびアドレスから名前への検索をサポートします。また、*view* ステートメントを使用することにより、1 つの DNS インスタンスが照会元 (インターネットやイントラネットなど) ごとに異なる内容で照会に応答できます。さらに、ジャーナル・ファイルを使用してゾーンの動的更新を保持します。

前の BIND 4.9.3 および BIND 8.2.5 はサポートされなくなっているため、BIND 9 にマイグレーションする必要があります。

新しい構成コマンド

システム上で以下の DNS 構成ファイルを管理しやすくするため、下記に示す構成コマンドが追加されました。

RNDC 構成の追加 (CRTRNDCCFG)

RNDC 構成ユーティリティ (CRTRNDCCFG) コマンドは、RNDC 構成ファイルの生成に使用します。このコマンドは、named.conf ファイル内で rndc.conf ファイルとそれに対応する制御ステートメントおよびキー・ステートメントを書き込む代わりに使用できる便利な方法です。

DNS 構成ユーティリティ (CHKDNSCFG)

DNS 構成ユーティリティ (CHKDNSCFG) コマンドは、`named.conf` という構成ファイルの構文を検査します。ただし、このコマンドではこの構成ファイルのセマンティクスを検査するサポートは提供されません。

DNS ゾーン・ユーティリティ (CHKDNSZNE)

DNS ゾーン・ユーティリティ (CHKDNSZNE) コマンドは、ゾーン・データ・ファイルの構文と整合性を検査します。ゾーン・データ・ファイルは DNS サーバーに追加する前に検査しておくことをお勧めします。

新しい照会および更新ユーティリティ

DNS サーバーの管理機能を強化するために、以下の照会および更新ユーティリティが追加されました。

Domain Information Groper (DIG)

DIG 照会ツールを使用して、ホスト、ドメイン、およびその他の DNS サーバーに関する情報を DNS サーバーの応答に基づいて検索することができます。またこのツールを使用して、DNS サーバーを使用できるようにシステムを構成する前に、その DNS サーバーが正しく応答しているかどうかを確認することもできます。

HOST 照会開始 (HOST)

HOST 照会開始 (HOST) コマンドは、DNS 検索用に使用します。このコマンドは、ドメイン名を IP アドレス (IPv4 または IPv6) に変換し、またその逆の変換も行います。

動的更新ユーティリティ (NSUPDATE)

動的更新ユーティリティ (NSUPDATE) コマンドは、Request for Comments (RFC) 2136 の定義に従って動的 DNS 更新要求を DNS サーバーに送信します。これにより、DNS サーバーの稼動中にリソース・レコードをゾーンに追加したり、ゾーンから除去したりすることができます。このため、手動でゾーン・ファイルを編集してレコードを更新する必要はありません。1 つの更新要求に複数のリソース・レコードを追加または除去するための要求を含めることはできますが、NSUPDATE コマンドによって動的に追加または除去されるリソース・レコードは同じゾーン内になければなりません。

Remote Name Daemon Control (RNDC)

Remote Name Daemon Control (RNDC) コマンドを使用して、システム管理者はネーム・サーバーの動作を制御することができます。このコマンドは `rndc.conf` という構成ファイルを読み取って、ネーム・サーバーとの接続方法を決定し、どのアルゴリズムとキーを使用すべきかを判断します。`rndc.conf` ファイルが見つからない場合、デフォルトによってインストール時に作成された `rndc-key_KID` ファイルが使用されます。このファイルはループバック・インターフェースを介して自動的にアクセスを許可します。

新規箇所または変更箇所を見つける方法

技術上の変更が加えられた箇所がわかるように、Information Center では以下を使用します。

- ➤ 記号は、新規の情報または変更された情報の開始点を示します。
- ⏪ 記号は、新規の情報または変更された情報の終了を示します。

PDF ファイルでは、新規情報および変更された情報の左マージンにリビジョン・バー (l) が記載されている場合があります。

関連資料

- | 9 ページの『BIND 9 の機能』
- | BIND 9 は BIND 8 と類似していますが、ドメイン・ネーム・システム (DNS) サーバーのパフォーマンスを向上するための機能 (ビューなど)をいくつか提供しています。

ドメイン・ネーム・システムの PDF ファイル

本書の PDF ファイルを表示および印刷することができます。


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. ご使用のブラウザの PDF リンクを右クリックします。
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。

関連資料

48 ページの『DNS の関連資料』

IBM Redbooks™ 資料、Web サイト、およびその他の Information Center のトピック・コレクションに、ドメイン・ネーム・システム (DNS) のトピック・コレクションに関連する情報が含まれています。PDF ファイルは、すべて表示または印刷が可能です。

ドメイン・ネーム・システムの概念

- | 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、ホストを見つけるときに IP アドレス (IPv4 の場合は 192.168.12.88 など、IPv6 の場合は 2001:D88::1 など) ではなく、www.jkltoys.com のような単純名を使用することができます。

1 つのサーバーは 1 つのゾーンのわずかな部分のホスト名と IP アドレスを知っているだけでよい場合がありますが、DNS サーバーは協同で働い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。DNS サーバーが協同して機能することにより、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なります。

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、照会を解決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

ドメイン・ネーム・システム (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。さらにそれらの各セットがそれぞれ固有のゾーン・タイプとなります。

- 1 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
- 1 す。1 つのゾーンに関する情報すべてを含んだサーバーは、そのドメインの権限サーバーです (親ゾーンと
- 1 呼びます)。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
- 1 に代行させる必要が生じます (子ゾーン と呼びます)。この場合、そのドメインに対する DNS サーバーは
- 1 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

i5/OS 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)、IPv4 アドレス (A)、IPv6 アドレス (AAAA)、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。

注: 2 次ゾーンは、他の BIND 資料で スレーブ・ゾーン と呼ばれる場合があります。

| 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』

ドメイン・ネーム・システム (DNS) クライアントは DNS サーバーを使用して照会を解決します。照会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。

関連タスク

34 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

17 ページの『例: イン트라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。

11 ページの『DNS リソース・レコード』

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。リソース・レコード参照表を使用して、i5/OS オペレーティング・システムでサポートされているリソース・レコードを調べることができます。

DNS 照会について

ドメイン・ネーム・システム (DNS) クライアントは DNS サーバーを使用して照会を解決します。照会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。

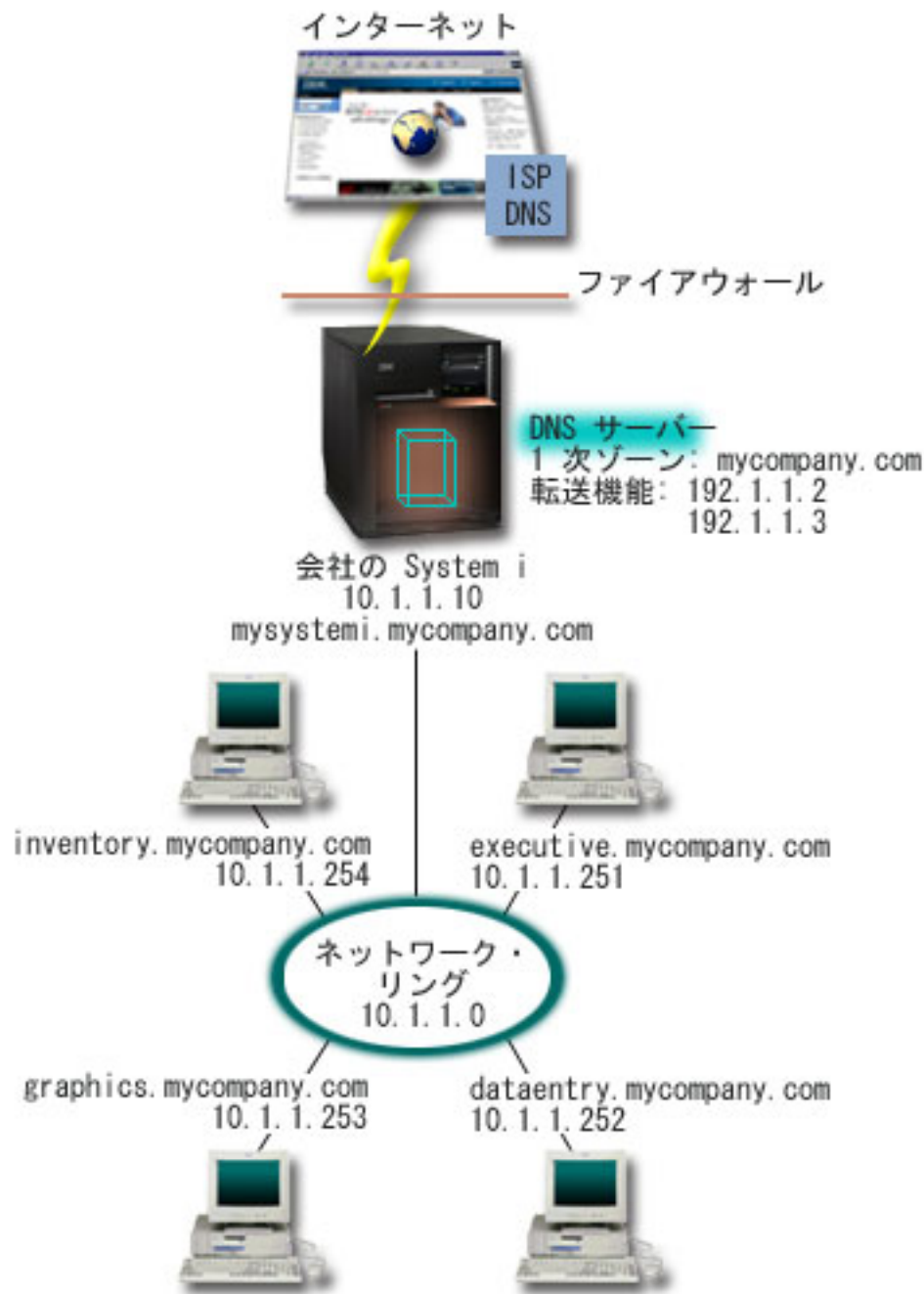


図1. インターネット・アクセスを行う単一 DNS サーバー

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。この場合にたどるパスは、再帰 または 反復 のいずれかが考えられます。DNS サーバーが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たうえで、その応答をクライアントに戻すことができます。さらに、要求側のサーバーは応答をそのキャッシュ内に保管して、次回このサーバーが同じ照会を受け取ったときにその応答を使用できるようにします。DNS サーバーが反復

1 | を使用するように設定されている場合、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
1 | ーへの連絡を試みることができます。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
1 | いて別個の追加照会を使用します。

関連資料

4 ページの『ゾーンについて』

ドメイン・ネーム・システム (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
れます。さらにそれらの各セットがそれぞれ固有のゾーン・タイプとなります。

19 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

ドメイン・ネーム・システム (DNS) ドメインのセットアップでは、他のユーザーが自分のドメイン名を使
用しないようにドメイン名を登録する必要があります。

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

19 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

BIND 9 に基づく i5/OS ドメイン・ネーム・システム (DNS) は動的更新をサポートします。動的ホスト構
成プロトコル (DHCP) などの外部ソースが DNS サーバーに更新を送信することができます。さらに、動
的更新ユーティリティー (NSUPDATE) などの DNS クライアント・ツールを使用して動的更新を実行する
こともできます。

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。しかし、BIND 8 以降に基づく DNS サーバーは、ゾーン・データの動的更新を求める他のソースからの要求を受け入れるように構成できるようになりました。

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 (IPv4 では A、IPv6 では AAAA) レコードまたは逆検索ポインター (PTR) レコード、あるいはこの両方を、クライアントに代わって更新できます。アドレス・マッピング・レコード (A または AAAA) 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、ネットワーク内の他のホストはクライアントの新 IP アドレスで DNS 照会することにより、クライアントを見つけることができます。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 (クライアントが IPv4 アドレスを使用している場合) または AAAA レコード (クライアントが IPv6 アドレスを使用している場合) 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、自身で A または AAAA レコードの更新要求を行うことをサポートしているとは限りません。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、単一の System i プラットフォーム上の DNS と DHCP の間、異なる System i プラットフォーム間、または System i プラットフォームと動的更新が可能な他のシステムとの間で実行できます。

- 注: 動的更新を DNS に送信するサーバー上には動的更新 DNS (QTOBUPDT) API が必要です。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。ただし、BIND 9 では、System i プラットフォームで更新を行う場合に NSUPDATE コマンドを使用する方法が推奨されます。

関連概念

動的ホスト構成プロトコル

関連タスク

35 ページの『動的更新を受信するためのドメイン・ネーム・システムの構成』

BIND 9 で実行されるドメイン・ネーム・システム (DNS) サーバーは、ゾーン・データの動的更新を

求める他の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 DNS に送信するための DHCP の構成

関連資料

21 ページの『例: ドメイン・ネーム・システムと動的ホスト構成プロトコルが同一の System i 上にある場合』

この例は、ドメイン・ネーム・システム (DNS) と動的ホスト構成プロトコル (DHCP) が同一の System i プラットフォーム上にある場合を示します。

11 ページの『DNS リソース・レコード』

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。リソース・レコード参照表を使用して、i5/OS オペレーティング・システムでサポートされているリソース・レコードを調べることができます。

QTOBUPT

『BIND 9 の機能』

BIND 9 は BIND 8 と類似していますが、ドメイン・ネーム・システム (DNS) サーバーのパフォーマンスを向上するための機能 (ビューなど)をいくつか提供しています。

| BIND 9 の機能

| BIND 9 は BIND 8 と類似していますが、ドメイン・ネーム・システム (DNS) サーバーのパフォーマンスを向上するための機能 (ビューなど)をいくつか提供しています。

| 単一の i5/OS DNS サーバー上におけるビュー

| `view` ステートメントを使用することにより、1 つの DNS インスタンスが照会元 (インターネットやイントラネットなど) ごとに異なる内容で照会に応答できます。

| 実際のビュー機能の 1 つの適用例として、複数の DNS サーバーを実行しなくても DNS のセットアップを分割できる点が挙げられます。例えば、1 つの DNS サーバー内で、内部ネットワークからの照会に応答するためのビューを 1 つ定義し、同時に、外部ネットワークからの照会に応答するためのビューをもう 1 つ別に定義することが可能です。

| 新しいクライアント・コマンド

| 以下のクライアント・コマンドにより、DNS サーバーの管理機能が向上します。

| 動的更新ユーティリティ (NSUPDATE)

| 動的更新ユーティリティ (NSUPDATE) コマンドを使用して、Request for Comments (RFC) 2136 の定義に従って動的 DNS 更新要求を DNS サーバーに送信します。これにより、DNS サーバーの稼動中にリソース・レコードをゾーンに追加したり、ゾーンから削除したりすることができます。このため、手動でゾーン・ファイルを編集してレコードを更新する必要はありません。1 つの更新要求に複数のリソース・レコードを追加または除去するための要求を含めることはできますが、NSUPDATE コマンドによって動的に追加または除去されるリソース・レコードは同じゾーン内になければなりません。

| 注: NSUPDATE コマンドを使用して、または DHCP サーバー経由で動的制御の対象となっているゾーンは、手動で編集しないでください。手動で編集した内容は動的更新の内容と競合する可能性があり、データ喪失の原因となります。

| DIG 照会開始 (DIG)

| Domain Information Groper (DIG) は、ネーム・サーバー検索 (NSLOOKUP) コマンドより機能が強化された照会ツールです。このツールは DNS サーバーから情報を検索するとき、または DNS サーバーの応答とテストするときで使用できます。NSLOOKUP コマンドは非推奨となっており、前のバージョンとの互換性確保のみを目的に提供されています。DIG を使用すると、DNS サーバーを使用できるようにシステムを構成する前に、その DNS サーバーが正しく応答しているか確認できます。また DIG を使用して、ホスト、ドメイン、およびその他の DNS サーバーに関する DNS 情報を検索することもできます。

| Domain Information Groper ツールを開始するには、DIG 照会開始 (STRDIGQRY) コマンドかその別名 DIG を使用します。

| HOST 照会開始 (HOST)

| HOST 照会開始 (HOST) コマンドは、DNS 検索用に使用します。このコマンドを使用して、ドメイン名を IP アドレス (IPv4 または IPv6) に変換し、またその逆の変換も行うことができます。

| Remote Name Daemon Control (RNDC)

| Remote Name Daemon Control (RNDC) コマンドは、システム管理者がネーム・サーバーの動作を制御できるようにする強力なユーティリティです。このコマンドは rndc.conf という構成ファイルを読み取って、ネーム・サーバーとの接続方法を決定し、どのアルゴリズムとキーを使用すべきかを判断します。

| rndc.conf ファイルが見つからない場合、デフォルトによってインストール時に作成された rndc-key._KID ファイルが使用されます。このファイルはループバック・インターフェースを介して自動的にアクセスを許可します。

| IPv6 のサポート

| BIND 9 は IPv6 の現在定義されているすべての形式で、名前からアドレスおよびアドレスから名前への検索をサポートします。順方向検索の場合、BIND 9 は AAAA と A6 の両方のレコードをサポートしますが、A6 レコードは非推奨となっています。IPv6 逆検索では ip6.arpa ドメインで使用されている従来の「ニブル」フォーマットをサポートし、古い、非推奨の ip6.int ドメインもサポートします。

| ジャーナル・ファイル

| ジャーナル・ファイルはゾーンの動的更新を保持するために使用します。このファイルは、クライアントから最初に動的更新を受け取ると自動的に作成され、消去されることはありません。これはバイナリー・ファイルであり、編集してはなりません。

| ジャーナル・ファイルがあると、シャットダウンや異常終了後に再始動されたサーバーはジャーナル・ファイルを再生して、最後のゾーン・ダンプ以降に行われたすべての更新をそのゾーンに取り込みます。ジャーナル・ファイルは、増分ゾーン転送 (IXFR) 方式で行われた更新の保管用にも使用されます。

| i5/OS用 DNS は BIND 9 を使用するように再設計されています。ご使用のシステムで BIND 9 DNS を実行するには、そのシステムが一定のソフトウェア要件を満たしていることが必要です。

| 関連概念

| 31 ページの『DNS の要件』

| ご使用の System i プラットフォームでドメイン・ネーム・システム (DNS) を実行するには、以下のソフトウェア要件を考慮してください。

| 7 ページの『動的更新』

| BIND 9 に基づく i5/OS ドメイン・ネーム・システム (DNS) は動的更新をサポートします。動的ホス

ト構成プロトコル (DHCP) などの外部ソースが DNS サーバーに更新を送信することができます。さらに、動的更新ユーティリティー (NSUPDATE) などの DNS クライアント・ツールを使用して動的更新を実行することもできます。

1 ページの『V6R1 の新機能』

ドメイン・ネーム・システム (DNS) のトピック・コレクションに対して新規追加された情報や大幅に変更された情報について説明します。

関連資料

23 ページの『例: 同一 System i 上に 2 つの DNS サーバーをセットアップしてファイアウォール上で DNS を分割する場合』

この例では、ファイアウォール上で作動するドメイン・ネーム・システム (DNS) サーバーを示します。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。この構成では、同一 System i プラットフォーム上に 2 つの DNS サーバーをセットアップすることで、こうした保護が実現されます。

30 ページの『セキュリティ基準の計画』

DNS には、いくつかのセキュリティ・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

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。リソース・レコード参照表を使用して、i5/OS オペレーティング・システムでサポートされているリソース・レコードを調べることができます。

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。

注: リソース・レコード参照表の項目は、BIND 資料の変更に応じて追加または除去されます。なお、これは BIND にリストされている全リソース・レコードを含む包括的リストではありません。

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。

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
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。
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 IPv6 アドレスを指定します。AAAA レコードは A レコードと類似しており、特定のドメイン名の IPv6 アドレスの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 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。

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・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。
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。

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
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。
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。
サービス・レコード	SRV	SRV レコードは、そのレコード内で定義済みのサービスをサポートするホストを指定します。このレコード・タイプは RFC 2782 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。

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
テキスト・レコード (Text records)	TXT	<p>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、ゾーンの責任者がど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。</p> <p>TXT レコードは、i5/OS 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 AS400DHCP という接頭部が付きまます。</p>
ウェルノウン・サービス・レコード (Well-Known Services records)	WKS	<p>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。</p>
X.400 アドレス・マッピング・レコード (X.400 Address Mapping records)	PX	<p>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。</p>
X25 アドレス・マッピング・レコード (X25 Address Mapping records)	X25	<p>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。</p>

関連概念

16 ページの『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

17 ページの『例: イン트라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。

4 ページの『ゾーンについて』

ドメイン・ネーム・システム (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。さらにそれらの各セットがそれぞれ固有のゾーン・タイプとなります。

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。

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・レコードの中の参照表には、i5/OS DNS がサポートするメール・レコードのタイプが記載されています。

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 レコードでのワイルドカード (例: *.mycompany.com) の使用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

11 ページの『DNS リソース・レコード』

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。リソース・レコード参照表を使用して、i5/OS オペレーティング・システムでサポートされているリソース・レコードを調べることができます。

例: ドメイン・ネーム・システム

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、System i プラットフォーム上で稼働する内部ネットワーク用の DNS を示しています。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。このシステムは「mycompany.com」ゾーン用の 1 次ネーム・サーバーです。

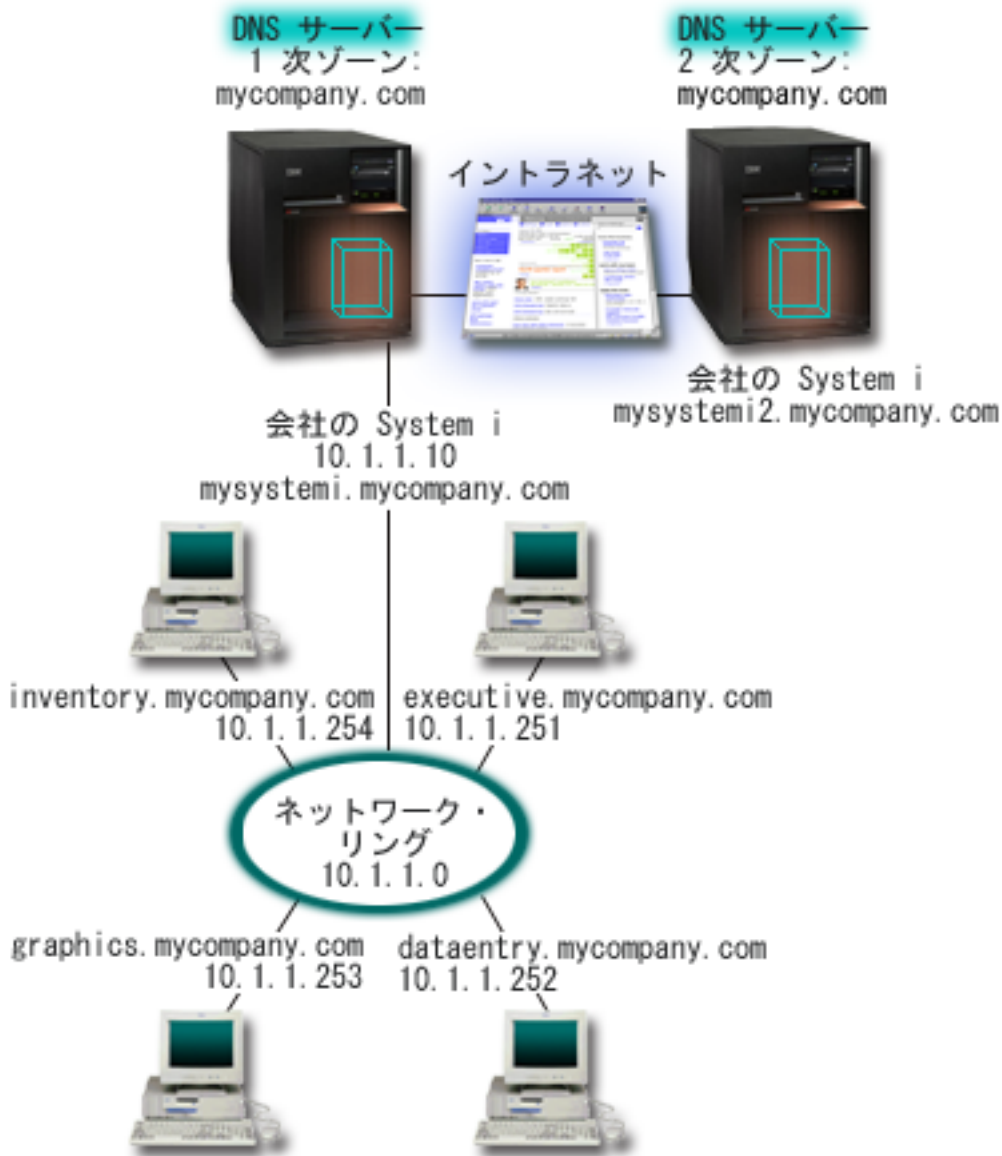


図2. イントラネット用の単一 DNS サーバー

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・レコード (IPv4 では A、IPv6 では AAAA) 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ます。

A、AAAA、および PTR レコードに加え、DNS は、ご使用のイントラネット上で他にどの TCP/IP ベース・アプリケーションが稼働しているかによって必要となる可能性のある、他の多数のリソース・レコードをサポートします。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。上記の図では、サーバー「mysystem1」はイントラネットの一部です。もう 1 つのシステム「mysystem2」は、mycompany.com ゾーンの 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

11 ページの『DNS リソース・レコード』

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。リソース・レコード参照表を使用して、i5/OS オペレーティング・システムでサポートされているリソース・レコードを調べることができます。

4 ページの『ゾーンについて』

ドメイン・ネーム・システム (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。さらにそれらの各セットがそれぞれ固有のゾーン・タイプとなります。

『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。

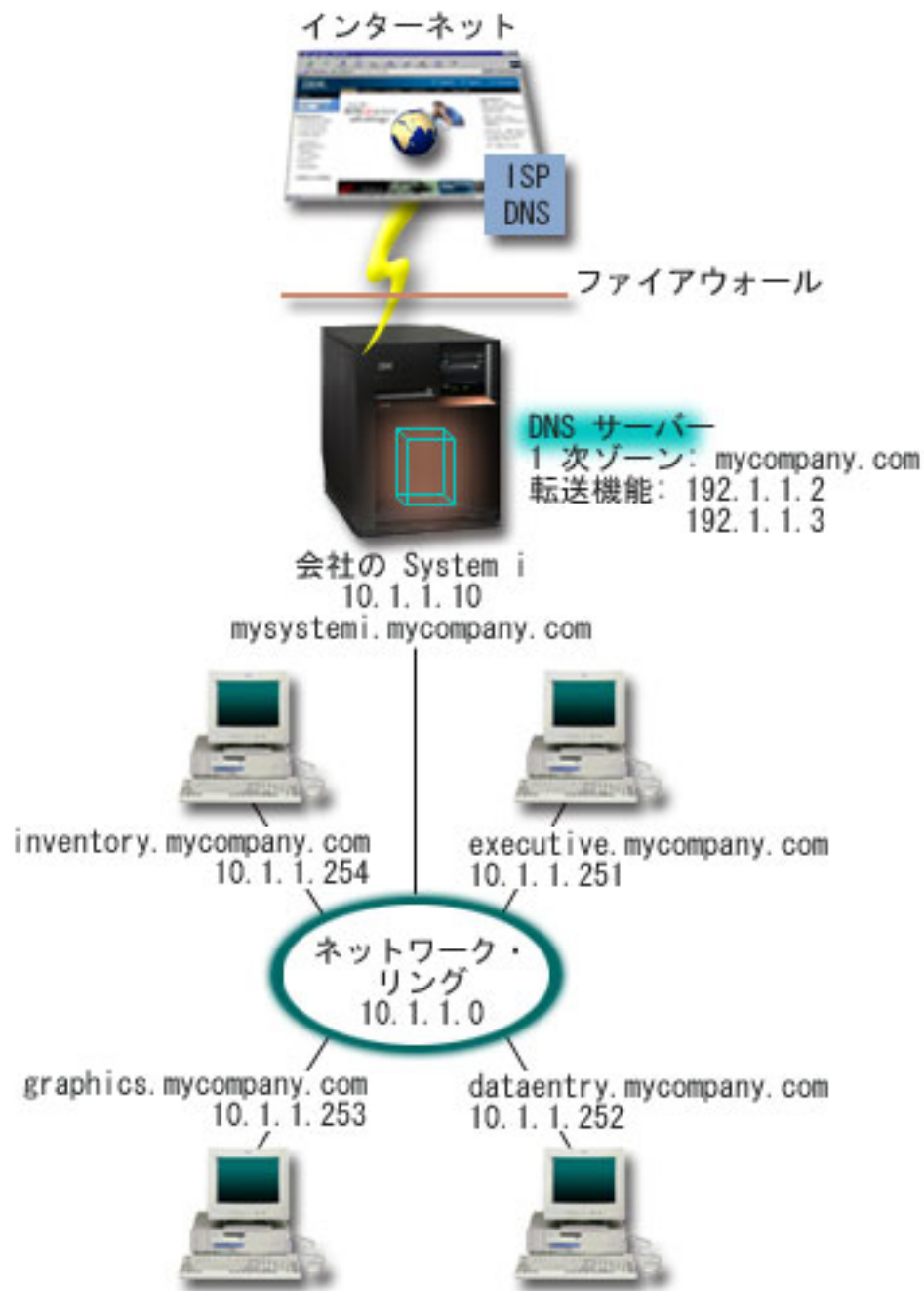


図3. インターネット・アクセスを行う単一 DNS サーバー

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、外部ドメイン・ネーム・システム・データへ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ク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 System i プラットフォームを保護してください。

関連概念

7 ページの『DNS ドメインのセットアップ』

ドメイン・ネーム・システム (DNS) ドメインのセットアップでは、他のユーザーが自分のドメイン名を使用しないようにドメイン名を登録する必要があります。

System i およびインターネット・セキュリティー

5 ページの『DNS 照会について』

ドメイン・ネーム・システム (DNS) クライアントは DNS サーバーを使用して照会を解決します。照会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。

関連資料

17 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: ドメイン・ネーム・システムと動的ホスト構成プロトコルが同一の System i 上にある場合

この例は、ドメイン・ネーム・システム (DNS) と動的ホスト構成プロトコル (DHCP) が同一の System i プラットフォーム上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。

次の図には、4 つのクライアントに対して DNS および DHCP サーバーとして機能する 1 つの System i プラットフォームを含む、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。

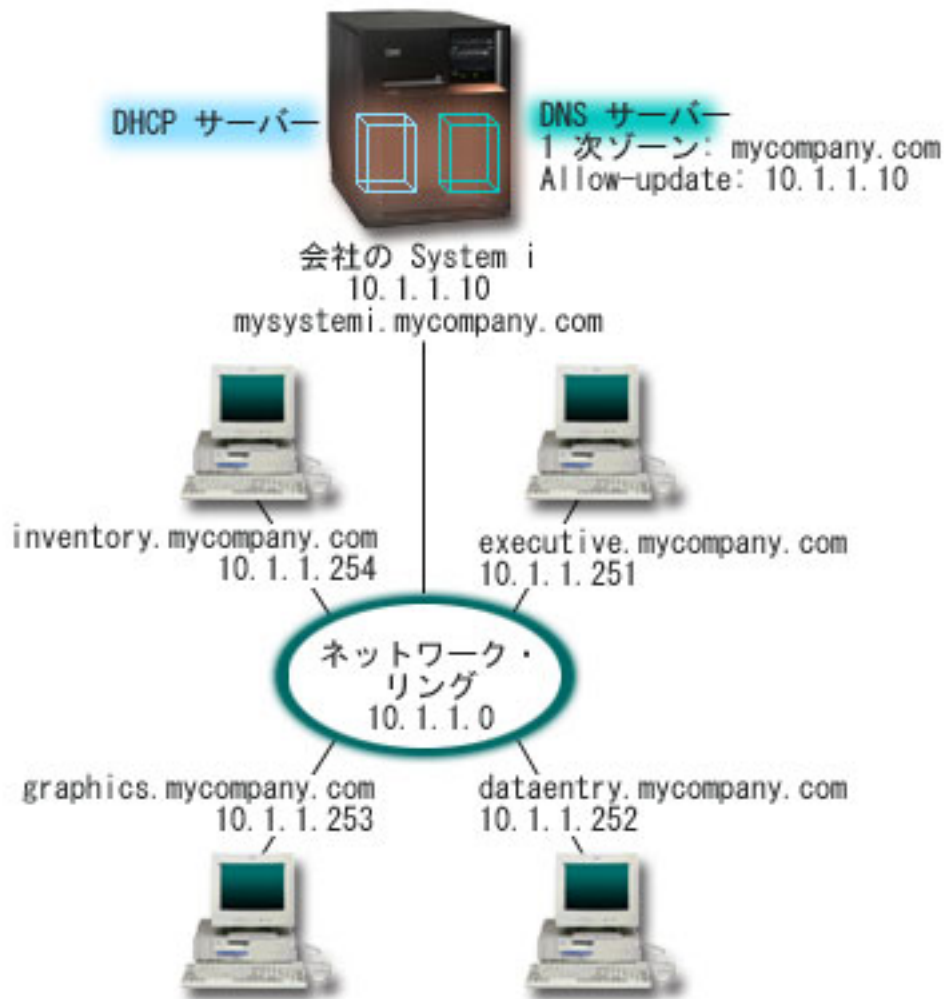


図4. DNS と DHCP が同一の System i プラットフォーム上にある場合

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す。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 9 に基づく i5/OS DNS サーバーでは、DHCP による断続的なアドレス変更に伴う DNS レコードへの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新し、DHCP により 10.1.1.250 という IP アドレスを割り当てられると、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、中断を起こさずに、それらのホスト名でグラフィックス・ファイル・サーバーについて DNS サーバー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あります。動的更新機能を使用するためのゾーンの構成について詳しくは、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

7 ページの『動的更新』

BIND 9 に基づく i5/OS ドメイン・ネーム・システム (DNS) は動的更新をサポートします。動的ホスト構成プロトコル (DHCP) などの外部ソースが DNS サーバーに更新を送信することができます。さらに、動的更新ユーティリティ (NSUPDATE) などの DNS クライアント・ツールを使用して動的更新を実行することもできます。

関連タスク

動的更新を DNS に送信するための DHCP の構成

関連資料

例: DNS と DHCP が異なる System i プラットフォームにある場合

例: 同一 System i 上に 2 つの DNS サーバーをセットアップしてファイアウォール上で DNS を分割する場合

この例では、ファイアウォール上で作動するドメイン・ネーム・システム (DNS) サーバーを示します。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。この構成では、同一 System i プラットフォーム上に 2 つの DNS サーバーをセットアップすることで、こうした保護が実現されます。

次の図には、セキュリティ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います。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、および外部から使用できる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。

| BIND 9 に基づく i5/OS DNS では、2 つの方法でこれを実現することができます。最初の方法は、その企
| 業が同一 System i プラットフォーム上に 2 つの DNS サーバー・インスタンス (1 つはイントラネット
| 用、もう 1 つはそのパブリック・ドメイン内のすべてのものが対象) をセットアップすることです。これ
| を次の例に示します。もう 1 つの方法は、BIND 9 で提供されるビュー機能を使用する方法です。これに
| ついては、ビューを使用してファイアウォール上で DNS を分割する状態を示す例の中で説明されていま
| す。

|

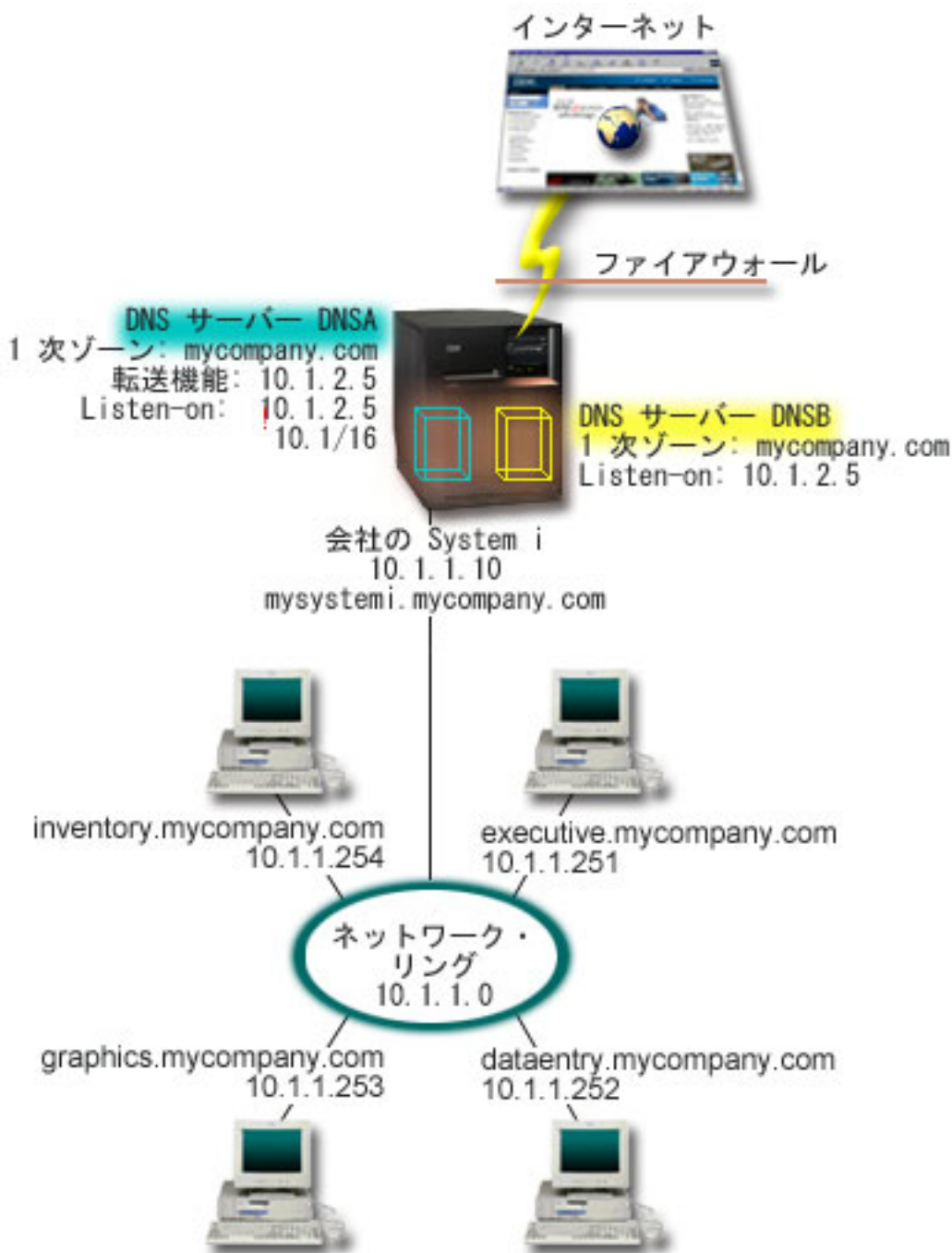


図5. 同一 System i 上に 2 つの DNS サーバーをセットアップしてファイアウォール上で DNS を分割する場合

外部サーバーの DNSB は、1 次ゾーン mycompany.com を使用して構成されています。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 を使用して構成されていますが、DNSA 上で定義されたゾーン・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 (forwarder) 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、DNSA サーバーのみを照会するように内部クライアントを構成する必要があります。DNS を分割するには、以下の構成設定を考慮する必要があります。

- Listen-on

他の DNS の例では、1 つの DNS サーバーのみが System i プラットフォーム上にあります。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。System i プラットフォーム上に複数の DNS サーバーがある場合は、必ず各サーバーが 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が 10.1.2.5 で送信されると仮定します。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 を除く 10.1.x.x インターフェース IP アドレス上のすべてのものから照会を受け入れるように構成されています。このアドレスを確実に除外するには、アドレス・マッチ・リストで、組み込み対象アドレスの接頭部の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.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てしまいます。サーバーは一致する最初の要素とそのアドレスを比較し、残りのルールをチェックせずにそのアドレスに許可を与えるためです。

関連資料

9 ページの『BIND 9 の機能』

BIND 9 は BIND 8 と類似していますが、ドメイン・ネーム・システム (DNS) サーバーのパフォーマンスを向上するための機能 (ビューなど)をいくつか提供しています。

『例: ビューを使用してファイアウォール上で DNS を分割する場合』

この例では、ファイアウォール上で作動するドメイン・ネーム・システム (DNS) サーバーを示します。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 BIND 9 が提供する view 機能を使用してインターネット上のデータにアクセスできます。

例: ビューを使用してファイアウォール上で DNS を分割する場合

この例では、ファイアウォール上で作動するドメイン・ネーム・システム (DNS) サーバーを示します。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 BIND 9 が提供する view 機能を使用して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います。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、および外部から使用できる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、ネットワークの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、内部ネットワークの外部からは利用できない特定の内部専用ゾーンに、その内部リゾルバーがアクセスできるようにしたいとも考えています。ただし、その企業はいかなる外側リゾルバーも内部ネットワークにアクセスできないようにすることを希望しています。

BIND 9 に基づく i5/OS DNS では、2 つの方法でこれを実現することができます。この例で説明する方法は、さまざまな照会を listen するために 2 つの異なるビュー (1 つはイントラネット用、もう 1 つはそのパブリック・ドメイン内のすべてのものが対象) を使用して DNS サーバーを構成できる、という方法です。もう 1 つの方法は、同一 System i プラットフォーム上に 2 つの DNS サーバー・インスタンスをセットアップする方法です。これについては、2 つの DNS サーバーを使用してファイアウォール上で DNS を分割する状態を示す例の中で説明されています。

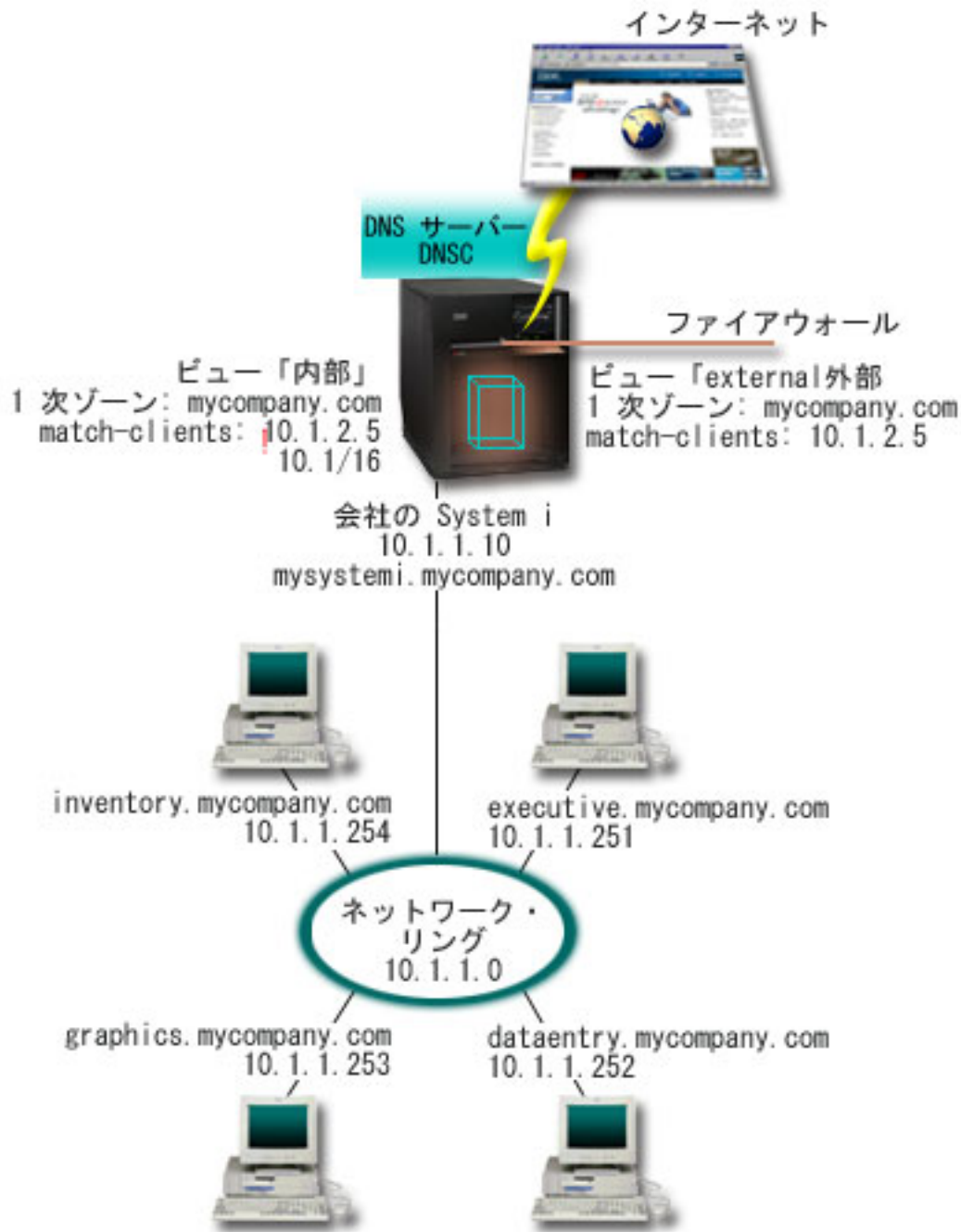


図 6. ビューを使用してファイアウォール上で DNS を分割する場合

1 DNS サーバーの DNSC は、外部 および内部 と呼ばれる 2 つのビューを定義します。外部 ビューは 1
1 次ゾーン mycompany.com を使用して構成され、このゾーンにはパブリック・ドメインに含めることを目的
1 としたリソース・レコードのみが含まれます。それに対し、内部 ビューは、イントラネット・リソース・
1 レコードを含む 1 次ゾーン mycompany.com を使用して構成されます。

1 ファイアウォールの保水性またはそれ以外のセキュリティ上の脅威が懸念される場合、内部データを保護
1 するために match-clients サブステートメントを使用するオプションがあります。このために、内部ホスト
1 から内部 mycompany.com ゾーンへの照会のみが許可されるように、内部ビューを構成することができま
1 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。

- 1 • match-clients

1 view ステートメントの match-clients は、引数としてアドレス・マッチ・リストを使用します。アドレ
1 ス・マッチ・リストと一致する照会の IP アドレスのみが、それを含む view の中で定義されている構成
1 値を見ることができます。照会の IP アドレスが、さまざまな view ステートメント内の複数の
1 match-clients 項目と一致した場合、最初の view ステートメントが適用されるステートメントとなりま
1 す。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が 10.1.2.5 で送信されると仮定しま
1 す。これらの照会は、外部ビュー内のゾーン・データが処理する必要があります。したがって、10.1.2.5
1 が外部ビューの match-clients となるように設定されます。内部ビューは、10.1.2.5 を除く 10.1.x.x イン
1 ターフェース IP アドレス上のすべてのものから照会を受け入れるように構成されています。このアドレ
1 スを確実に除外するには、アドレス・マッチ・リストで、組み込み対象アドレスの接頭部の前に除外対
1 象アドレスをリストしておく必要があります。

- 1 • アドレス・マッチ・リストの順序

1 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、
1 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)
1 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
1 否認されます。

1 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
1 てしまいます。サーバーは一致する最初の要素とそのアドレスを比較し、残りのルールをチェックせず
1 にそのアドレスに許可を与えるためです。

1 関連資料

1 23 ページの『例: 同一 System i 上に 2 つの DNS サーバーをセットアップしてファイアウォール上で
1 DNS を分割する場合』

1 この例では、ファイアウォール上で作動するドメイン・ネーム・システム (DNS) サーバーを示しま
1 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
1 のデータにアクセスできます。この構成では、同一 System i プラットフォーム上に 2 つの DNS サ
1 ーバーをセットアップすることで、こうした保護が実現されます。

ドメイン・ネーム・システムの計画

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
キュリティなどのサブジェクトを評価する必要があります。

ドメイン・ネーム・システム権限の決定

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。

管理者が DNS の構成と管理を行うには、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してをお勧めします。ユーザーに権限を与えるには、System i ナビゲーターを使用します。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」というトピック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

40 ページの『ドメイン・ネーム・システム構成ファイルの維持管理』

i5/OS DNS を使用して、System i プラットフォーム上で DNS サーバー・インスタンスを作成および管理することができます。DNS の構成ファイルは System i 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 System i ナビゲーターを使用して行ってください。

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。

i5/OS DNS には、システム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、以下の項目を覚えておくと便利です。

- System i プラットフォーム上で定義されたすべてのゾーンおよびオブジェクトは、「前方参照ゾーン」および「逆引き参照ゾーン」というフォルダー内に編成されます。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 および AAAA 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。
- i5/OS 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。

セキュリティ基準の計画

DNS には、いくつかのセキュリティ・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。

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・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・リスト項目の順序

指定されたアドレスと一致するアドレス・マッチ・リスト中の最初の項目が使用されます。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・リストの項目は (!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 は最初の項目と比較され、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。サーバーは一致する最初の項目とそのアドレスを比較し、残りのルールをチェックせずにそのアドレスに許可を与えるためです。

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。

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上の考慮事項以外にも、DNS のセキュリティおよび System i のセキュリティについては、System i プラットフォ

ームおよびインターネットのトピック・コレクションなど、さまざまな資料で取り上げられています。
「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。

関連概念

System i およびインターネット・セキュリティー

関連資料

9 ページの『BIND 9 の機能』

BIND 9 は BIND 8 と類似していますが、ドメイン・ネーム・システム (DNS) サーバーのパフォーマンスを向上するための機能 (ビューなど)をいくつか提供しています。

DNS の要件

ご使用の System i プラットフォームでドメイン・ネーム・システム (DNS) を実行するには、以下のソフトウェア要件を考慮してください。

DNS 機能、オプション 31 は、オペレーティング・システムと一緒に自動的にインストールすることはありません。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。i5/OS 用に追加された DNS サーバーは、BIND 9 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 8.2.5 を基にしており、引き続き i5/OS で使用できます。

DNS をインストールした後は、BIND 4 または 8 から BIND 9 に DNS サーバーをマイグレーションして構成する必要があります。さらに i5/OS PASE もインストールされている必要があります。これは i5/OS のオプション 33 です。i5/OS PASE がインストールされると、System i ナビゲーターは現在の 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。

別のプラットフォームで動的ホスト構成プロトコル (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にしたい場合は、その DHCP サーバーにオプション 31 もインストールされていることが必要です。DHCP サーバーは、オプション 31 によって提供されるプログラミング・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

i5/OS PASE

32 ページの『ドメイン・ネーム・システムの構成』

System i ナビゲーターを使用して、ネーム・サーバーを構成し、自分のドメイン以外の場所で照会を解決することができます。

関連資料

9 ページの『BIND 9 の機能』

BIND 9 は BIND 8 と類似していますが、ドメイン・ネーム・システム (DNS) サーバーのパフォーマンスを向上するための機能 (ビューなど)をいくつか提供しています。

ドメイン・ネーム・システムがインストールされているかどうかの判別

ドメイン・ネーム・システム (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. 「5761SS1 ドメイン・ネーム・システム」 (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」になっています。

LicPgm	Installed Status	Description
5761SS1	*COMPATIBLE	Domain Name System

4. 「F3」を押して表示を終了します。

ドメイン・ネーム・システムのインストール

ドメイン・ネーム・システム (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。

ドメイン・ネーム・システムの構成

System i ナビゲーターを使用して、ネーム・サーバーを構成し、自分のドメイン以外の場所で照会を解決することができます。

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

31 ページの『DNS の要件』

ご使用の System i プラットフォームでドメイン・ネーム・システム (DNS) を実行するには、以下のソフトウェア要件を考慮してください。

System i ナビゲーター でのドメイン・ネーム・システムへのアクセス

以下の手順では、System i ナビゲーターで DNS 構成インターフェースに進みます。

i5/OSPASE を使用している場合、BIND 9 に基づいて DNS サーバーを構成することができます。

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. System i ナビゲーターで、**ご使用のシステム** → 「ネットワーク」 → 「サーバー」 → 「DNS」を展開します。
2. 「DNS」を右クリックし、「新規構成」を選択します。

関連概念

System i ナビゲーター入門

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 9 ベースの i5/OS 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。

複数の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、以下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

40 ページの『ドメイン・ネーム・システム構成ファイルの維持管理』

i5/OS DNS を使用して、System i プラットフォーム上で DNS サーバー・インスタンスを作成および管理することができます。DNS の構成ファイルは System i 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 System i ナビゲーターを使用して行ってください。

ネーム・サーバー・インスタンスの作成

「新規 DNS 構成」ウィザードを使用すると、DNS サーバー・インスタンスを定義するためのプロセスを順を追って実行していくことができます。

「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. System i ナビゲーターで、**ご使用のシステム** → 「ネットワーク」 → 「サーバー」 → 「DNS」を展開します。
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. ウィザードの指示に従って、構成プロセスを完了します。

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 サーバーの名前を指定します。この名前は 5 文字までの長さで、英字 (A から Z) 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、それらのインスタンスをすべての IP アドレスで listen するように構成することはできません。そうしないと、それらのインスタンスを同時に実行できません。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: インターネットにアクセスできる状態にあり、ご使用の DNS がインターネット名を完全に解決できるものと予想している場合は、デフォルトのインターネット・ルート・サーバーのロードのみ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。

ドメイン・ネーム・システム・サーバー・プロパティの編集

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を編集するには、以下のステップに従ってください。

1. System i ナビゲーターで、**ご使用のシステム** → 「ネットワーク」 → 「サーバー」 → 「DNS」を展開します。
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」を選択します。
4. 目的のプロパティを編集します。

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。

サーバー上のゾーンを構成するには、以下のステップを実行してください。

1. System i ナビゲーターで、**ご使用のシステム** → 「ネットワーク」 → 「サーバー」 → 「DNS」を展開します。
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」のいずれかのフォルダーを右クリックして、作成したいゾーン・タイプを選択します。
4. ウィザードの指示に従って、作成プロセスを完了します。

関連概念

36 ページの『外部ドメイン・ネーム・システム・データへのアクセス』

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

35 ページの『動的更新を受信するためのドメイン・ネーム・システムの構成』

BIND 9 で実行されるドメイン・ネーム・システム (DNS) サーバーは、ゾーン・データの動的更新を求める他の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。

35 ページの『ドメイン・ネーム・システム・ファイルのインポート』

ドメイン・ネーム・システム (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

4 ページの『ゾーンについて』

ドメイン・ネーム・システム (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。さらにそれらの各セットがそれぞれ固有のゾーン・タイプとなります。

1 ネーム・サーバー上のビューの構成

1 BIND 9 が提供する機能の 1 つが view ステートメントです。これにより、1 つのドメイン・ネーム・システム (DNS) インスタンスが照会元 (インターネットやイントラネットなど) ごとに異なる内容で照会に
1 応答できます。実際のビューの 1 つの適用例として、複数の DNS サーバーを実行しなくても DNS のセ
1 ットアップを分割できる点が挙げられます。

1 サーバー上でビューを構成するには、以下のステップを実行してください。

1. System i ナビゲーターで、**ご使用のシステム** → 「ネットワーク」 → 「サーバー」 → 「DNS」を展開
1 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、「ビュー (Views)」を右クリックし、「新規ビュー (New View)」を選択します。
4. ウィザードの指示に従って、作成プロセスを完了します。

動的更新を受信するためのドメイン・ネーム・システムの構成

BIND 9 で実行されるドメイン・ネーム・システム (DNS) サーバーは、ゾーン・データの動的更新を求める他の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必要がある場合、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と、そのサーバーが最初にゾーン・データベースからそのゾーン・データをロードした時点以降に行われたすべての動的更新を使用して、強制的にゾーン・データベースが更新されます。サーバーを停止しない場合、ゾーン・データベースに手動で行った更新は実行中のサーバーによって上書きされるため、すべて失われます。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. System i ナビゲーターで、**ご使用のシステム** → 「ネットワーク」 → 「サーバー」 → 「DNS」を展開します。
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」を選択します。
5. 「1 次ゾーン・プロパティ」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・リストの項目タイプを選択し、「追加」をクリックします。追加できる項目は、IP アドレス、IP 接頭部、アクセス制御リスト、またはキーです。
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。

関連タスク

34 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。

動的更新を DNS に送信するための DHCP の構成

ドメイン・ネーム・システム・ファイルのインポート

ドメイン・ネーム・システム (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。

BIND 構文に基づく有効なゾーン構成ファイルであるゾーン・データ・ファイルをインポートすることにより、1 次ゾーンを作成することができます。このファイルは Integrated File System 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、指定されたサーバー・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. System i ナビゲーターで、**ご使用のシステム** → 「ネットワーク」 → 「サーバー」 → 「DNS」を展開します。
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. 「DNS 構成」ウィンドウの左側のペインで「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。

関連タスク

34 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・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。

外部ドメイン・ネーム・システム・データへのアクセス

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回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。

System i ナビゲーターのデフォルトのルート・サーバーのリスト

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、System i ナビゲーターにあります。そのリストは、System i 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

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. 匿名メソッド (FTP.INTERNIC.NET または RS.INTERNIC.NET) でファイル転送プロトコル (FTP) を使用して InterNIC サーバーにログオンします。
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: /QOpenSys/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。

関連タスク

34 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。

ドメイン・ネーム・システムの管理

ドメイン・ネーム・システム (DNS) サーバーの管理作業には、DNS 機能が正しく機能しているかどうかの検証、パフォーマンスのモニター、および DNS データおよびファイルの維持管理が含まれます。

ドメイン・ネーム・システムが正しく機能しているかどうかの検証

- | Domain Information Groper (DIG) ツールは、ドメイン・ネーム・システム (DNS) サーバーから情報を収集し、その応答をテストするときに利用できます。DIG を使用すると、DNS サーバーが正しく機能しているかどうかを検証することができます。
- | 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こともできます。これにより、テストしている特定のサーバー・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。
- | DIG を使用して 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、DIG HOSTNAME('127.0.0.1') REVERSE(*YES) と入力します。

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。

```
;; global options: printcmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id:865
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL:1

;; QUESTION SECTION:
;1.0.0.127.in-addr.arpa.      IN      PTR

;; ANSWER SECTION:
1.0.0.127.in-addr.arpa.  86400  IN      PTR  localhost.

;; AUTHORITY SECTION:
0.0.127.in-addr.arpa.   86400  IN      NS    ISA2LP05.RCHLAND.IBM.COM.

;; ADDITIONAL SECTION:
ISA2LP05.RCHLAND.IBM.COM. 38694  IN      A     9.5.176.194

;; Query time: 552 msec
;; SERVER: 9.5.176.194#53(9.5.176.194)
;; WHEN: Thu May 31 21:38:12 2007
;; MSG SIZE rcvd: 117
```

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。

2. セッションを終了するには、「Enter」を押します。

注: DIG の使用に関するヘルプが必要な場合は、?DIG と入力して「Enter」を押します。

セキュリティ・キーの管理

セキュリティ・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 に関連するキーは、DNS キーと動的更新キーの 2 つのタイプがあります。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。

ドメイン・ネーム・システム・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. System i ナビゲーターで、**ご使用のシステム** → 「ネットワーク」 → 「サーバー」 → 「DNS」を展開します。
2. 右側のペインで、管理したい 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。

「キーの管理」ウィンドウで、対応する管理作業を実行することができます。

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、ドメイン・ネーム・システム (DNS) と DHCP が同じ System i プラットフォーム上に
- | ある場合に必要になります。DHCP が異なる System i プラットフォーム上にある場合は、権限サーバー
- | に動的更新を送信する必要がある各リモート System i プラットフォームに同じ動的更新キー・ファイルを
- | 配布しなければなりません。配布は、FTP、E メールなどを介して行います。

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. System i ナビゲーターで、**ご使用のシステム** → 「ネットワーク」 → 「サーバー」 → 「DNS」を展開します。
 2. 「DNS」を右クリックし、「動的更新キーの管理」を選択します。
- | これで、「動的更新キーの管理」ウィンドウで、対応する管理作業を実行することができます。

ドメイン・ネーム・システム・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

40 ページの『ドメイン・ネーム・システム構成ファイルの維持管理』

i5/OS DNS を使用して、System i プラットフォーム上で DNS サーバー・インスタンスを作成および管理することができます。DNS の構成ファイルは System i 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 System i ナビゲーターを使用して行ってください。

サーバー統計の使用

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. System i ナビゲーターで、**ご使用のシステム** → 「ネットワーク」 → 「サーバー」 → 「DNS」を展開します。
 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。
- | Remote Name Daemon Control (RNDC) コマンドを使用して、named.stats ファイル内のサーバー統計情報
 - | を表示することもできます。これに対応するコマンドは以下です。

- | `RNDC RNDCCMD('stats')`

アクティブ・サーバー・データベースへのアクセス

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 (権限付与の開始 (SOA) 情報など)、および全ホスト・プロパティ (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。

System i 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、i5/OS ディレクトリー・パス (`/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. System i ナビゲーターで、**ご使用のシステム** → 「ネットワーク」 → 「サーバー」 → 「DNS」を展開します。
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。

| Remote Name Daemon Control (RNDC) コマンドを使用して、`named_dump.db` ファイル内のアクティブ・サーバー・データベース情報を表示することもできます。これに対応するコマンドは以下です。



| `RNDC RNDCCMD('dumpdb -all')`

ドメイン・ネーム・システム構成ファイルの維持管理








i5/OS DNS を使用して、System i プラットフォーム上で DNS サーバー・インスタンスを作成および管理することができます。DNS の構成ファイルは System i 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 System i 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: 下記のファイル構造は、BIND 9 で稼働する DNS に適用されます。

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
<code>/QIBM/UserData/OS400/DNS/</code>		DNS 用の開始点ディレクトリー。
<code>/QIBM/UserData/OS400/DNS/<instance-n>/</code>		DNS インスタンス用の開始点ディレクトリー。

名前	アイコン	説明
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。
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 9 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 9 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.conf		このファイルには構成データが含まれます。管理対象となっている特定ゾーン、ゾーン・ファイルの場所、動的に更新できるゾーン、その転送サーバーの場所、およびその他のオプション設定をサーバーに知らせます。
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.memstats		サーバー・メモリー統計 (named.conf で構成されている場合)。
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。
named.random		サーバー生成のエントロピー・ファイル。
named.recurring		再帰的なサーバー照会 (System i ナビゲーターによって要求された場合)。
named.run		デフォルト・デバッグ・ログ (要求された場合)。named.run.0、named.run.1 などとしてロールオーバーできます。
named.stats		サーバー統計。

名前	アイコン	説明
<primary-zone-n>.db		これはこのサーバー上の特定のドメインの 1 次ゾーン・ファイルです。このファイルには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。
<primary-zone-n>.jnl		ゾーンの動的更新を保持するジャーナル・ファイル。これは最初に動的更新を受け取ったときに作成されます。シャットダウンや異常終了後に再始動されたサーバーはジャーナル・ファイルを再生して、最後のゾーン・ダンプ以降に行われたすべての更新をそのゾーンに取り込みます。このファイルは、増分ゾーン転送 (IXFR) 用にも使用されます。これらのログ・ファイルは消去されることはありません。これはバイナリー・ファイルであり、編集してはなりません。
db.<secondary-zone-n>		このサーバー上の特定のドメインの 2 次ゾーン・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。このファイルは、1 次サーバーが到達不能である場合に、始動時に 2 次サーバーを最初にロードするときに使用されます。各ゾーンには個別の .db ファイルがあります。
/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-n>._KEY		<key_id-n> キーを持つ DNSSEC キーへの .Symlink。これは常に、最後に作成される K<key_id-n>.+aaa+nnnnn.key キーを指します。
<key_id-x>._DUK. <zone-a>		<key_id-x> キーを使用して <zone-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-x>._KID		<key_id-x> という名の key_id でキー・ステートメントを含むファイル。
<key_id-y>._DUK. <zone-a>		<key_id-y> キーを使用して <zone-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-y>._DUK. <zone-b>		<key_id-y> キーを使用して <zone-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。
<key_id-y>._KID		<key_id-y> という名の key_id でキー・ステートメントを含むファイル。

名前	アイコン	説明
<code>rndc-confgen.random.nnnnnn</code>		さまざまなコマンド (エントロピー・ファイルが必要とするもの) 用のエントロピー・ファイル。 <code>nnnnn</code> 部分は、このファイルを作成したジョブのジョブ番号です。何らかの理由でコマンドが取り消されても、これらのファイルはそのまま残され、クリーンアップされません。

関連概念

28 ページの『ドメイン・ネーム・システム権限の決定』

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についても検討する必要があります。

39 ページの『ドメイン・ネーム・システム・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

32 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。

System i ナビゲーター において、DNS は DNS サーバーを構成および管理するための拡張機能を持つインターフェースを提供します。 i5/OS グラフィカル・インターフェースに精通した管理者向けに、以下のタスクがショートカットとして提供されます。これらのタスクにより、複数のインスタンスのサーバー状況および属性を同時に変更できる迅速な方法が提供されます。

関連タスク

47 ページの『ドメイン・ネーム・システムの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。

ドメイン・ネーム・システム・サーバーの始動または停止

System i ナビゲーター インターフェース内のドメイン・ネーム・システム (DNS) で複数のサーバー・インスタンスを同時に始動または停止できない場合、文字ベース・インターフェースを使用すると、これらの設定を複数のインスタンスで同時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

大規模ゾーンを持っている管理者が、サーバーが最初に始動してすべてのゾーン・データをロードしているときに大量のデバッグ・データが収集されることを避けたい場合は、デバッグ・レベルを変更することをお勧めします。

System i ナビゲーター・インターフェース内では、ドメイン・ネーム・システム (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・インターフェースを使用すると、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・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、コマンド内の *nnnnn* をサーバー・インスタンス名に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 だけ上げるには、`RNDC RNDCCMD('trace')` と入力して「Enter」を押します。
 - | • デバッグをオフにするには、`RNDC RNDCCMD('notrace')` と入力して、「Enter」を押します。

ドメイン・ネーム・システムのトラブルシューティング

ドメイン・ネーム・システム (DNS) のロギングおよびデバッグ設定値を、DNS サーバーで発生した問題の解決に役立てることができます。

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 9 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、後に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。

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 9 にはいくつかのロギング・オプションがあります。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。一般にはデフォルトのロギング設定値は適切ですが、設定を変更する場合は、BIND 9 に関する他の資料でロギングに関する情報を参照することをお勧めします。

ロギング・チャンネル

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

ファイル・チャンネル

ファイル・チャン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・チャンネルは `i5os_debug` と `i5os_QPRINT` です。デフォルトにより、デバッグ・メッセージは `i5os_debug` チャンネルに記録されます。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。 `i5os_QPRINT` に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ンネルの他に、自分自身のファイル・チャンネルを作成できます。

SYSLOG チャンネル

このチャンネルに記録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 チャンネルは `i5os_joblog` です。このチャン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・チャンネル

ヌル・チャンネルに記録されたメッセージはすべて廃棄されます。デフォルトのヌル・チャンネルは `i5os_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・チャン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。各チャン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。そのカテゴリーを以下に示します。

client クライアント要求の処理。

config 構成ファイルの構文解析と処理。

database

ゾーン・データおよびキャッシュ・データを保管するために DNS サーバーが内部的に使用するデータベースに関連するメッセージ。

default 特定の構成が定義されていないカテゴリーのロギング・オプションの定義。

delegation-only

代行のみ (delegation-only)。これは、ヒント・ゾーンまたはスタブ・ゾーン宣言に `delegation-only` ゾーンまたは `delegation-only` が指定されたために、強制的に NXDOMAIN とされた照会を記録します。

dispatch

着信パケットのサーバー・モジュール (それらのパケットが処理される場所) へのディスパッチング。

dnssec DNS Security Extensions (DNSSEC) および Transaction Signature (TSIG) プロトコルの処理。

general

他のどのカテゴリーにも分類できないメッセージに使用される汎用カテゴリー。

lame-servers

リモート・サーバー内で構成が間違っている不良サーバー。BIND 9 が解決中にそれらのサーバーを照会しようとしてこれを検出します。

| network

| ネットワーク操作。

| **notify** NOTIFY プロトコル。

| resolver

| キャッシュ・ネーム・サーバーがクライアントに代わって実行する、再帰検索などの DNS 解決。

| security

| 要求の承認または拒否。

| **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。

| unmatched

| 指定されたメッセージで、一致するビューがなかったクラスを判別できませんでした。1 行の要約が **client** カテゴリにも記録されます。このカテゴリはほとんどの場合、ファイルまたは標準エラー出力に送信されます。デフォルトでは、ヌル・チャンネルに送信されます。

| **update** 動的更新。

| update-security

| 更新要求の承認または拒否。照会では照会を記録する場所が指定されます。始動時にカテゴリ照会を指定すると、**querylog** オプションが指定されていない限り、照会ロギングが有効になります。

| 照会ログ項目では、クライアントの IP アドレスとポート番号、照会名、クラス、およびタイプが報告されます。また、**Recursion Desired** フラグが設定されたかどうか (設定されている場合は +、設定されていない場合は -)、EDNS が使用されているか (E)、または照会が署名されているかどうか (S) も報告されます。

| ログ・ファイルはサイズが大きくなる可能性があり、定期的に削除することが可能です。DNS ログ・ファイルの内容は、DNS サーバーを停止して始動するとすべてクリアされます。

メッセージ重大度

チャンネルは、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。各チャンネルごとに、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、チャンネルは警告、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

ログイン・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. System i ナビゲーターで、**ご使用のシステム** → 「ネットワーク」 → 「サーバー」 → 「DNS」を展開します。
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」を選択します。
4. 「サーバー・プロパティ」ウィンドウで「チャンネル」タブを選択します。これは、新規のファイル・チャンネルまたはチャンネルのプロパティ（各チャン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」ウィンドウで、「ログイン」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ンネルにログ出力されるかを指定するためです。

重大度レベルに関するトラブルシューティングのヒント

i5os_joblog チャン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ときは、場合により重大度レベルの変更が必要になります。上記の手順に従って「チャンネル」ページにアクセスし、i5os_joblog チャン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。これで、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らします。

ドメイン・ネーム・システムの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。通常ログインによって容易に問題を発見できますが、場合によってはデバッグが必要になります。通常の状態では、デバッグはオフ（値を 0 にする）にします。まず最初にログイン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 以上の値を指定すると、デバッグ情報が i5/OS ディレクトリー・パス (/QIBM/UserData/OS400/DNS/<server instance>) にある named.run ファイルに書き込まれます。パスの <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 以上に設定され、DNS サーバーが実行を続ける限り、拡大し続けます。「サーバー・プロパティ」- 「チャンネル」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設定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. System i ナビゲーターで、**ご使用のシステム** → 「ネットワーク」 → 「サーバー」 → 「DNS」を展開します。
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」を選択します。
4. 「サーバー・プロパティ - 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

43 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。

DNS の関連資料







IBM Redbooks 資料、Web サイト、およびその他の Information Center のトピック・コレクションに、ドメイン・ネーム・システム (DNS) のトピック・コレクションに関連する情報が含まれています。PDF ファイルは、すべて表示または印刷が可能です。

IBM Redbooks

AS/400® TCP/IP Autoconfiguration: DNS and DHCP Support  (5181 KB)

この Redbooks 資料には、i5/OS に組み込まれているドメイン・ネーム・システム (DNS) サーバーおよび動的ホスト構成プロトコル (DHCP) サーバーのサポートの説明が記載されています。この資料に記載されている情報は、例を使って DNS および DHCP サポートをインストール、調整、構成、およびトラブルシューティングするときに役立ちます。

Web サイト

- | • *DNS and BIND* (第 5 版)。Paul Albitz および Cricket Liu。O'Reilly and Associates, Inc. 発行。 
| Sebastopol, California, 2006。ISBN 番号: 0-59610-057-4。
- | • Internet System Consortium (ISC)  Web サイトから入手する BIND 管理者用リファレンス・マニュアル (PDF 版)。
- | • 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維持管理しています。
- | • 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。

関連資料

3 ページの『ドメイン・ネーム・システムの PDF ファイル』
本書の PDF ファイルを表示および印刷することができます。

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。

〒106-8711
東京都港区六本木 3-2-12
IBM World Trade Asia Corporation
Intellectual Property Law & 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を提供し、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。

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。

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。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認できません。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ます、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 (ドメイン・ネーム・システム (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。

AS/400
i5/OS
IBM
IBM (ロゴ)

Adobe、Adobe ロゴ、PostScript、PostScript ロゴは、Adobe Systems Incorporated の米国およびその他の国における登録商標または商標です。

他の会社名、製品名およびサービス名等はそれぞれ各社の商標です。

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を提供され、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