ドメイン ネーム システムの概要

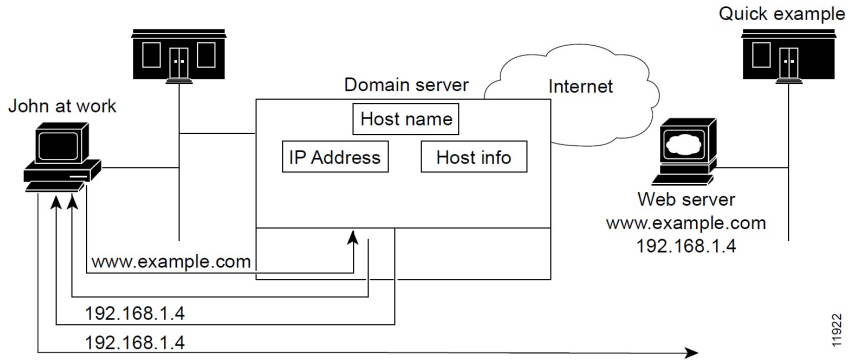
ドメイン ネーム システム（DNS）は増加するインターネットユーザーに対応しています。DNS は www.cisco.com などの名前を 192.168.40.0 などの IP アドレス（または拡張 IPv6 アドレス）に変換して、コンピュータが互いに通信できるようにします。DNS は、World Wide Web などのインターネットアプリケーションを使いやすくします。このプロセスは、友人や親戚に電話をかける時に、相手の電話番号を覚えていなくても、相手の名前を使って自動的にダイヤルすることができます。

DNS の仕組み

DNS の仕組みを理解するために、ユーザーの典型である John が自分のコンピュータにログインしていると仮定してください。John は ExampleCo 社の Web サイトを表示するために Web ブラウザを起動します（以下の図を参照）。Web サイト名 http://www.example.com を入力します。次のアクションを実行します。

1. John のワークステーションは、www.example.com の IP アドレスに関する要求を DNS サーバーに送信します。
2. DNS サーバーがデータベースをチェックして、www.example.com が 192.168.1.4 に対応していることを確認します。
3. サーバーは、このアドレスを John のブラウザに返します。
4. ブラウザは、このアドレスを使用して Web サイトを見つけます。
5. John のモニターのブラウザにこの Web サイトが表示されます。

Figure 1: ドメイン名とアドレス



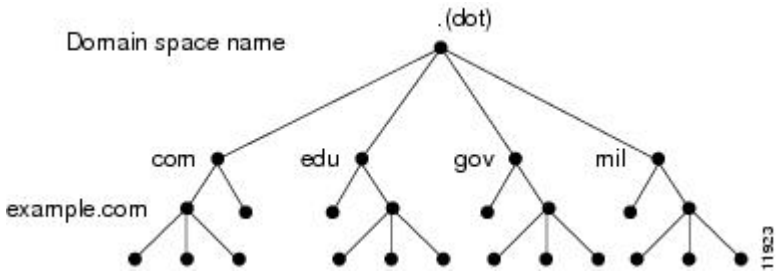
DNS の概念の概要

ここでは、DNS に関する概念について説明します。

ドメイン

John は、DNS サーバーが www.example.com の IP アドレスを認識しているため、ExampleCo の Web サイトにアクセスできます。サーバーは、ドメイン名前空間を検索してアドレスを学習しました。DNS はツリー構造として設計されており、各ネームド ドメインはツリー内のノードです。ツリーの最上位のノードは DNS ルートドメイン（.）です。その下に .com、.edu、.gov、.mil といったサブドメインがあります（以下の図を参照）。

図 *2 : DNS* 階層

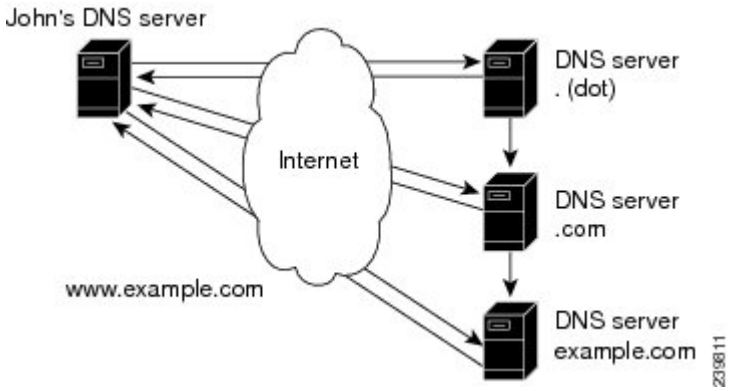


完全修飾ドメイン名（FQDN）は、ルートに戻るすべてのネットワーク ドメインのドット区切りの文字列です。この名前は、インターネット上のホストごとに一意です。ドメイン例の FQDN、example.com. の場合は、ドメインは example、親ドメインは .com、ルート ドメインは「.」（ドット）です。

ExampleCo アドレスの調査

John のワークステーションが Web サイト www.example.com の IP アドレスを要求した場合（以下の図を参照）：

図 *3 : DNS* 階層名の検索



1. ローカル DNS サーバーがデータベース内で www.example.com ドメインを検索しますが、そのドメインを見つけることができません。これは、このサーバーがこのドメインに対する権威ではないことを意味しています。
2. このサーバーは権威ルート ネームサーバーに最上位レベル（ルート）ドメイン「.」（ドット）を要求します。
3. ルート ネームサーバーは、サブドメインを認識している .com ドメインのネームサーバーにクエリを送信します。
4. .com ネームサーバーは、example.com がサブドメインの 1 つであることを確認して、そのサーバー アドレスで応答します。
5. ローカル サーバーは、example.com ネームサーバーに www.example.com のロケーションを要求します。
6. example.com ネームサーバーは、そのアドレスが 192.168.1.4 であると応答します。
7. ローカルサーバーは、このアドレスを John の Web ブラウザに送信します。

ドメインの確立

ExampleCo には John が到達できる Web サイトがあります。ExampleCo のドメインが認定ドメイン レジストリに登録されているからです。ExampleCo は、.com サーバー データベースにもドメイン名を入力し、IP アドレスの範囲を定義するネットワーク番号を要求しました。

この場合のネットワーク番号は 192.168.1.0 です。これには、192.168.1.1 ～ 192.168.1.254 の範囲内の割り当て可能なホストがすべて含まれています。各アドレス フィールドには、0 ～ 255（28）の数字のみを使用できます。これはオクテットと呼ばれます。ただし、番号 0 ～ 255 はネットワーク アドレスとブロードキャスト アドレス用にそれぞれ予約されており、ホストには使用されません。

ドメインとゾーンの違い

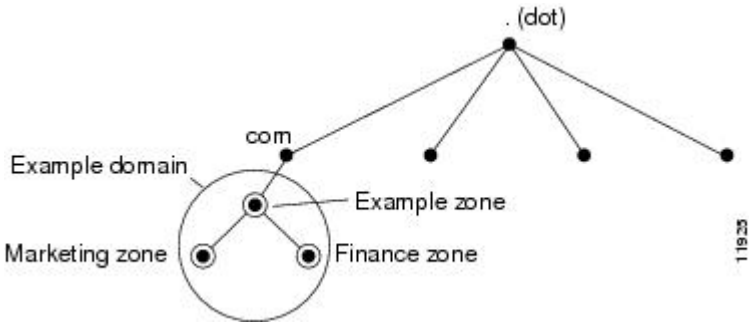
ドメイン名前空間は、DNSツリーの委任ポイントである、ゾーンと呼ばれるエリアに分割されます。ゾーンには、他のゾーンが権威であるドメインを除いて、特定のポイント以下のすべてのドメインが含まれます。

大抵のゾーンには権威ネームサーバーがあります（複数あることが多い）。組織内で多くのネームサーバーを使用できますが、インターネット クライアントはルート ネームサーバーが認識しているネームサーバーのみをクエリできます。他のネームサーバーは、内部クエリだけに応答します。

ExampleCo 社はドメイン example.com を登録しました。example.com、marketing.example.com、finance.example.com という 3 つのゾーンを確立しました。ExampleCo は社内のマーケティング グループと財務グループの DNS サーバーに marketing.example.com と finance.example.com の権限を委任しました。marketing.example.com のホストについて example.com にクエリすると、example.com はそのクエリを marketing.example.com ネームサーバーに送信します。

次の図では、ドメイン example.com に 3 つのゾーンが含まれています。example.com ゾーンは自己に対する権威でしかありません。

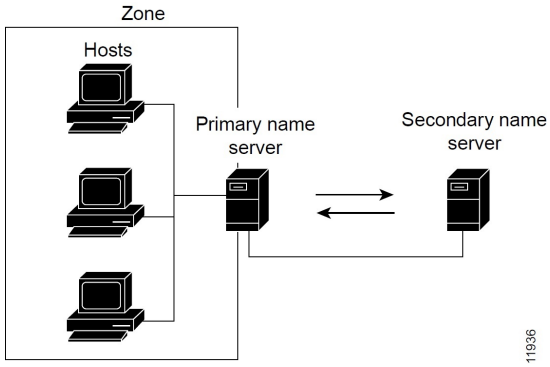
図 *4:* 委任されたサブドメインを含む *example.com*



ExampleCo にはサブドメインに権限を委任しないという選択肢もありました。その場合には、example.com ドメインはマーケティングと財務のサブドメインに対して権威のあるゾーンです。example.com サーバーは、マーケティングと財務に関するすべての外部クエリに応答します。

Cisco Prime Network Registrar を使用してゾーンの設定を開始する際には、ゾーンごとにネームサーバーを設定する必要があります。各ゾーンには 1 台のプライマリ サーバーがあり、そのサーバーがローカル コンフィギュレーション データベースからゾーン コンテンツをロードします。各ゾーンには、任意の数のセカンダリ サーバーを含めることができます。セカンダリ サーバーはプライマリ サーバーからデータを取得して、ゾーン コンテンツをロードします。次の図は、セカンダリ サーバーが 1 台である場合の構成を示しています。

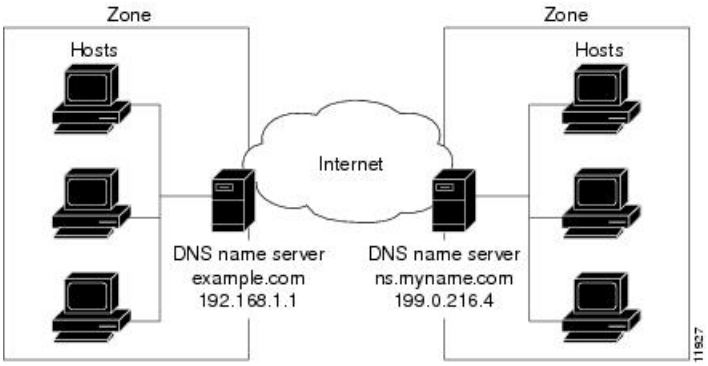
図 *5:* ゾーンのプライマリ サーバーとセカンダリ サーバー



ネームサーバー

DNS は、クライアント/サーバー モデルに基づいています。このモデルでは、ネームサーバーは DNS データベースの一部に関するデータを保存し、ネットワーク上のネームサーバーに照会するクライアントにそのデータを提供します。ネームサーバーは、物理ホスト上で実行されるプログラムであり、ゾーンデータを保存します。ドメインの管理者は、ゾーン内のホストを記述するすべてのリソースレコード（RR）のデータベースを使用してネームサーバーをセットアップします（下図を参照）。

Figure 6: クライアント/サーバー名の解決



DNS サーバーは、名前をアドレスに変換するか、名前を解決します。これらのサーバーは FQDN の情報を解釈してそのアドレスを見つけます。

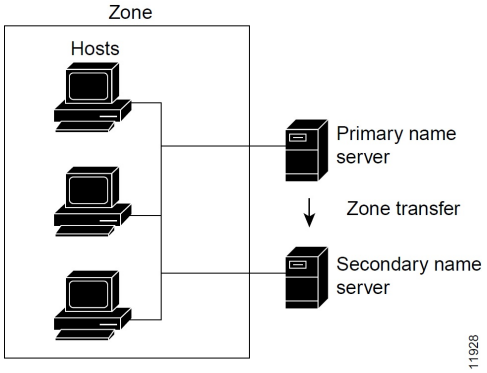
各ゾーンには、ローカル データベースからゾーン コンテンツをロードする 1 台のプライマリ ネームサーバーと、プライマリ サーバーからのデータのコピーをロードする多数のセカンダリ サーバーが必要です（以下の図を参照）。プライマリ サーバーからセカンダリ サーバーを更新するこのプロセスは、ゾーン転送と呼ばれます。

セカンダリ ネームサーバーはプライマリ サーバーへのバックアップとして機能しますが、両方のタイプのサーバーがゾーンに対する権威を持っています。両方とも、クエリへの応答時に得た情報からではなく、ゾーンの権威データベースからゾーン内のホスト名を認識します。クライアントは、両方のサーバーに対して名前の解決を照会できます。

Cisco Prime Network Registrar DNS ネームサーバーを設定する際には、ゾーンに対するサーバーのロール（プライマリ、セカンダリ、またはキャッシュ専用）を指定します。サーバーのタイプは、そのロールのコンテキストでのみ意味があります。権威 DNS サーバーは、ゾーンのプライマリサーバーまたはセカンダリサーバーにのみにすることができ、キャッシングサーバーのゾーンは指定しません。

Cisco Prime Network Registrar では、権威サービスとキャッシュサービスは分離され、2 つの個別サーバーで処理されます。権威サーバーは、権威ゾーンデータを保持し、自己の権威が及ぶクエリにのみ応答します。キャッシュ サーバーは、再帰/キャッシュ サーバーであり、権威ゾーン データを含みません。

***Figure 7: DNS* ゾーン転送**



設定方法：

- プライマリ ネームサーバーの設定については、「プライマリ DNS サーバーの管理」を参照してください。
- セカンダリ ネームサーバーの設定については、「セカンダリ サーバーの管理」を参照してください。

逆引きネームサーバー

これまで説明した DNS サーバーは、名前からアドレスへの解決を実行します。これは、データベース内で正しいアドレスを検索することで簡単に実行できます。すべてのデータが名前でインデックス化されるためです。ただし、特定の出力（コンピュータ ログ ファイルなど）を解釈できるように、アドレスから名前への解決が必要な場合があります。

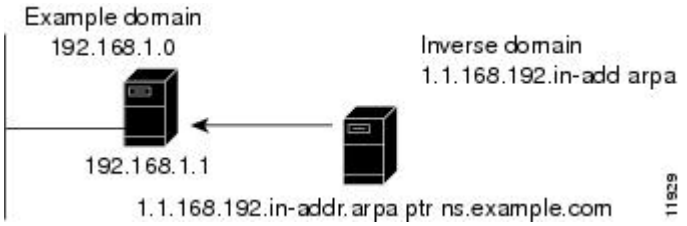
アドレスのみがわかっている場合にドメイン名を検索するには、名前空間全体を検索する必要があります。DNS は、アドレスを名前として使用するドメイン名前空間（in-addr.arpa または .arpa ドメイン）をサポートすることで、この問題を解決します。この逆引きゾーンには、ネットワーク番号に基づく各ネットワークのサブドメインが含まれます。整合性と自然なグループ化を実現するた めに、ホスト番号の 4 つのオクテットが逆順に並べられます。

IP アドレスをドメイン名として読み取ると、その名前はリーフからルートという逆順に表示されます。たとえば、ExampleCo のドメイン ネットワーク番号は 192.168.1.0 です。その逆引きゾーンは 1.168.192.in-addr.arpa. です。DNS サーバーアドレス（192.168.1.1）のみがわかってい

る場合は、逆ドメインへのクエリによって、example.com にマッピングされるホスト エントリ 1.1.168.192.in-addr.arpa を得られます。

逆ドメインは、次の図に示すように、ポインタ（PTR）RR によって処理されます。

Figure 8: 逆ドメイン



権威 DNS サーバーとキャッシュ DNS サーバー

DNS サーバー機能が拡張されて、許可用とキャッシュ用に個別の DNS サーバーが提供されるようになりました。この機能拡張により、Cisco Prime Network Registrarは DNS64、DNSSEC、ドメイン リダイレクト、フル IPv6 をサポートし、キャッシュ パフォーマンスが向上しました。

ハイ アベイラビリティ DNS

ゾーンごとに 1 つのプライマリ DNS サーバーしか存在できないため、このサーバーに障害が発生すると、ゾーン データを更新できなくなります。これらの更新は、プライマリ DNS サーバーでのみ発生する可能性があります。DNS リソースレコードを更新するソフトウェア（DHCP サーバーなど）は、更新をプライマリサーバーに直接送信する必要があります。2 つ目のプライマリサーバーは、メインのプライマリサーバーをシャドーイングするホットスタンバイにすることができます。これはハイ アベイラビリティ（HA）DNS と呼ばれます。

EDNS

User Datagram Protocol（UDP）を介して 512 バイトを超える DNS メッセージを送信するには、拡張 DNS（EDNS）という DNS プロトコルの拡張を使用する必要があります。EDNS プロトコルは、DNS プロトコルで使用可能なフラグ、ラベル タイプ、および戻りコードの数を増やします。RFC 6891 で定められている EDNS のバージョンは EDNS0 と呼ばれています。EDNS は OPT リソース レコード（OPT RR）という疑似リソース レコードを使用します。OPT RR は通常の DNS と EDNS を区別します。OPT RR は DNS クライアントとサーバーの間のルート伝送にのみ出現します。キャッシュされたり、ディスクに保存されたりすることはありません。DNS パケットを EDNS としてマークする DNS エンドポイントは、DNS 要求または応答の追加データ セクションに OPT RR を挿入する必要があります。

権威サーバーとキャッシング DNS サーバーは、EDNS0 拡張をサポートしますが、オプション コード はサポートしていません。DNS サーバーの UDP ペイロード サイズを変更できます。DNS サーバーの最小 UDP ペイロード サイズは 512 バイトです。UDP パケットの最大サイズは 64 KB です。キャッシングサーバーのデフォルトサイズは 1,232 KB です。

Note DNS サーバーは、EDNS0 をサポートしていないクライアントからの要求を処理できますが、EDNS0 をサポートしていないクライアントからの要求を処理するときに拡張機能は使用できません。クライアント要求に対する応答は、デフォルトの 512 バイトのメッセージに挿入されます。クライアントは、クエリに OPT RR を含めることによって、EDNS をサポートしていることを示している場合があります。サーバーが EDNS をサポートしていない場合（またはサポートが無効になっている場合）、サーバーは FORMERR を返し、クライアントは EDNS を使用せずに再試行します。クライアントが報告したサイズ（EDNS 使用またはデフォルトの 512 バイト）を超える応答の場合は、サーバーは結果を省略としてマークし、クライアントは TCP を使用して再試行できます。

Note IP フラグメンテーションは、特に大規模な DNS メッセージが発生した場合に、インターネット上で問題となります。フラグメンテーションが動作している場合でも、DNS に十分なセキュリティが確保されていない可能性があります。これらの問題は、次のいずれかの方法で修正できます。a) EDNS バッファ サイズを低く設定して、IP フラグメンテーションのリスクを軽減する、b) DNS 応答が大きすぎて制限したバッファ サイズでは修正できない場合、DNS を UDP から TCP に切り替える。キャッシュ DNS サーバーと権威 DNS サーバーの両方でデフォルトの EDNS バッファ サイズが 4096 バイトの場合は、値を小さく（1232 バイト）することで IP フラグメンテーションを防ぐことができます。

EDNS バッファ サイズを設定するには、次のコマンドを使用します。

権威 DNS サーバー：

```
nrcmd> session set visibility=3
nrcmd> dns set edns-max-payload=1232
nrcmd> dns reload
```

キャッシュ DNS サーバー：

```
nrcmd> session set visibility=3
nrcmd> cdns set edns-buffer-size=1232
nrcmd> cdns set max-udp-size=1232
nrcmd> cdns reload
```

DNS ビュー

DNS ビューでは、単一のネームサーバーを使用してゾーンデータの代替バージョンを異なるクライアントのコミュニティに表示できます。

たとえば、example.com の DNS サーバーは、ゾーンの 2 つのビューを維持できます。内部で照会できる example.com のビューには、外部ビューに存在しない多数のホストが含まれています。各ゾーン ビューは、ゾーンの独立したコピーとして扱われます。DNS サーバーは、ゾーンに関するクエリに応答するときに、各ビューで定義されている一致基準を使用して、クライアントの一致ゾーンを見つけます。その後、そのゾーン コンテンツに基づいてクエリに応答します。ゾーン コンテンツがビュー間でわずかに異なる場合があります。