CHAPTER 1

GSS の導入

この章では、Cisco Global Site Selector（GSS）について説明すると同時に、GSS デバイスの理解と操作に欠かせない、役立つ用語および概念を紹介します。

この章の主な内容は、次のとおりです。

GSS に適用する DNS ベースの Global Server Load Balancing（GSLB; グローバル サーバ ロード バランシング）の詳細については、次の Cisco.com の URL から入手できる『*Business Case for Global Server Load Balancing*』ホワイト ペーパーを参照してください。

http://www.cisco.com/en/US/product/hw/contnetw/ps4162/prod_white_papers_list.html

GSS の概要

企業の LAN またはインターネットへの接続に使われる Cisco Content Services Switch（CSS）や Cisco Content Switching Module（CSM）のような Server Load Balancing（SLB; サーバ ロード バランシング）デバイスは、同様のコンテンツを含む複数のサーバ間にコンテンツ要求を分散させます。SLB デバイスを使用すると、コンテンツ参照者は、その要求を処理するために最適なホストに転送されます。

世界中に支店を持つ組織や、サービスを提供する Web やアプリケーションを取り扱うグローバルなビジネス組織には、地理的に分散された複数のバックアップを持つデータセンターにルーティングを行うため、複雑な要求を実行できるネットワーク デバイスが必要です。これらのネットワーク デバイスには、グローバルにサーバの負荷を分散し、高速な応答や障害復旧、フェールオーバー保護を実行する機能、つまり GSLB が必要です。

Cisco GSS プラットフォームを使用すると、分散およびミラーリングされた複数のデータセンターにグローバルにコンテンツを配置できます。こうすることで最適なサイトを選択したり、Domain Name System（DNS; ドメイン ネーム システム）応答を改善したり、データセンターのアベイラビリティを確保したりできます。

GSS は従来からの DNS ルーティング階層に挿入されます。また、データセンターの SLB 状態や負荷を監視するために、Cisco CSS や Cisco CSM、またはサードパーティ製の SLB と密接に連携します。GSS はこれらの情報やユーザ指定のルーティング アルゴリズムを使用して、最適でもっとも負荷の少ないデータセンターを即座に選択します。

GSS はサイトの停止状態を検出できるため、Web ベースのアプリケーションは常にオンライン状態を保つことができます。突然オフラインになったデータセンターにユーザが要求を送信した場合でも、その要求は使用可能なリソースに迅速に再ルーティングされます。

GSS は、ドメイン ネーム スペース部のドメイン解決プロセスを制御し、1 秒間に数千の要求に応答することで、従来の DNS サーバのタスクを軽減します。

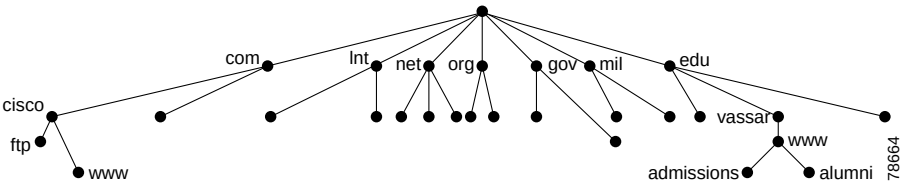
DNS ルーティング

ここでは、GSS の背景にある主要な DNS ルーティングの概念について説明します。

1980 年代のはじめ以降、インターネット上のコンテンツ ルーティングの処理には、DNS（ドメイン名を IP アドレスにマッピングするホスト情報の分散データベース）が使用されてきました。電子メール、Telnet などのリモート端末アクセス、FTP（ファイル転送プロトコル）によるファイル転送、Web サーフィンなど、インターネットで発生するほとんどすべてのトランザクションに DNS が使用されています。DNS は、ホストのコンテンツに関係ない数値表記の IP アドレスでなく、覚えやすいアルファベット表記のホスト名を使用します。

DNS ではドメイン ネーム スペースと呼ばれるほぼ無制限のホスト名を管理できます（図 1-1）。また、DNS を使用すると、データベース全体のセグメント（個々のドメイン）をローカルに管理できるだけでなく、ネットワーク全体からそのセグメント内のデータを使用できます。このプロセスのことを*委任*と呼びます。

図 1-1　　ドメイン ネーム スペース



DNS ネーム サーバ

ドメイン ネーム スペースの情報は、インターネット中に分散されているネーム サーバに格納されています。各サーバは、ドメイン ネーム スペース全体のわずか一部分に関する完全な情報を格納しています。このスペースのことを*DNS ゾーン*と呼びます。ゾーン ファイルには 1 つのドメイン（「mycompany.com」）またはサブドメイン（「gslb.mycompany.com」）に関する情報が含まれています。DNS 情報はリソース レコードと呼ばれる情報行で構成されています。

リソース レコードには、ゾーンのグローバル プロパティおよびそのゾーンを構成するホストやサービスが記載されています。これらはバイナリ形式で内部的に保存され、DNS ソフトウェアに使用されます。ただし、ゾーン転送時は、ネットワークにテキスト形式で送信されます。

リソース レコードは次のレコード タイプをはじめ、さまざまなものから構成されています。

- Start of Authority（SOA）
- Name Service（NS）
- Address（A）
- Host Information（HINFO）
- Mail Exchange（MX）
- Canonical Name（CNAME）
- Pointer（PTR）

このマニュアルでは、主に SOA と NS レコード タイプを説明します。リソース レコードの設定手順や他のサポートされているレコード タイプの詳細については、『*Cisco CNS Network Registrar User's Guide*』を参照してください。また、リソース レコードの背景の詳細については RFC 1034 および 1035 を参照してください。

ここでは、次の内容を説明します。

SOA レコード

ドメインのトップレベルのネーム データベースには、そのドメイン内のデータに対してもっとも信頼のおける情報元を示した SOA レコードが含まれている必要があります。また、SOA レコードにも現在の DNS データベース バージョンが含まれており、特定の DNS サーバの動作を定義しています。

別々にネーム サービスされる各サブドメインには、少なくとも対応する NS レコードが 1 つ含まれている必要があります。ネーム サーバはこれらのレコードを使用してお互いを検出します。ゾーンは別々の SOA を持つネーム スペースの領域です。このレコード形式の例を次に示します。

```
DOMAIN.NAME. IN SOA Hostname.Domain.Name. Mailbox.Domain.Name.
1 ; serno (serial number)
86400 ; refresh in seconds (24 hours)
7200 ; retry in seconds (2 hours)
2592000 ; expire in seconds (30 days)
345600 ; TTL in seconds (4 days)
```

ネガティブ キャッシング

多忙なサーバは、1 秒間に何百、何千もの名前解決要求を処理する必要があります。そのため、実装されている DNS サーバには、効率性を向上させるために、解決に時間とリソースが奪われる不要な名前解決要求を切り捨てるためのメカニズムが必要になります。このような要求でも、データ転送ビジネスで使用するインターネットワークの帯域幅を消費します。

キャッシングは、これらの効率性を維持するメカニズムのうち、もっとも重要なものの 1 つです。キャッシングとは、新しく取得した情報を、再利用できるように別途保存しておくためのメモリ領域のことです。DNS の場合、新しく名前解決した結果やその他の要求を保存するために DNS のネーム サーバがキャッシングを使用します。そうすることで、同じ要求が発生した際に、他の名前解決処理の要求をわざわざ発生させなくても、キャッシュを使用してその要求を満たすことができます。詳細については、「要求解決」セクションを参照してください。

ネガティブ キャッシングはネーム サーバ内の機能で、存在していない特定の DNS レコードを管理します。ネガティブ キャッシングは負の結果を保存することで、負の回答に対する応答時間を削減します。また、このキャッシングを使用することでリゾルバとネーム サーバ間のメッセージ数を削減できるため、ネットワーク全体のトラフィック量も削減できます。ネガティブ キャッシュの状態を管理すれば、システムはルックアップ処理が再実行されるときも、障害状態から迅速に復帰できます。

SOA レコード内の Time to Live（TTL）フィールドは、情報を更新するために、ネーム サーバが互いにポーリングを行う頻度を制御します。具体的には、TTL フィールドは、データのキャッシュ時間を決定するためにネーム サーバが互いにポーリングする頻度を制御します。DNS は TTL を使用して、ネーム サーバに負の結果の配信を、リゾルバに負の結果のキャッシュを許可します。

DNS クエリーに対して負の応答を形成する場合、Resource Record Set（RRset）やドメイン ネームが存在しない、または回答を提供できないという情報をネガティブ キャッシングが保存しているため、SOA レコードの TTL が必要です。

（注）　RRset は、同じラベル、クラス、およびタイプを含み、かつ異なるデータを保有するレコード グループです。

もっとも一般的な負の応答として、特定の RRset が DNS に存在していない場合があげられます。応答コード（RCODE）フィールドに、*name error* が記述されることでネーム エラー（NXDOMAIN）が示されます。また、NOERROR に送信された RCODE の回答に NODATA が示され、answer セクションに回答に関連するものがないことが伝えられます。このような負の応答の場合、GSS はそのゾーンの SOA レコードを応答の authority セクションに追加します。

SOA レコードおよび負の応答

SOA レコードを負の応答に含める必要がある場合、GSS はこれに対応するネーム サーバに、対応するドメインの SOA の問い合わせを実行します。この SOA 応答は、SOA レコードの minimum フィールドで指定された期間、キャッシュされます。この期間中のすべての負の応答に対してキャッシュされた SOA レコードが使用されます。同じドメインのネーム サーバに問い合わせることはありません。

（注）　GSS v2.0 のデフォルトの動作では、クエリーに対して負の応答を返す設定になっていますが、GSS v1.3.3 のデフォルトの動作では、負のクエリーには応答しない設定になっています。

GSS が SOA を取得できなかった場合、負の応答は該当するエラー コードになります。キャッシュされている SOA を使用すると、SOA がキャッシュされたときから負の応答の TTL が秒単位で減少します。このプロセスは、キャッシュ専用のネーム サーバがキャッシュされたレコードの TTL を減少させる方法と類似しています。

（注） 新しい DNS 機能が不要で、クエリーに対する負の応答タイプにこだわらずに GSS v2.0 にアップグレードする場合、追加の SOA 設定を実行する必要はありません。そのような場合、GSS は、要求に答えられないときに SOA 情報を持たないタイプ 3 の負の応答を戻します。

GSS で負の応答に使用する SOA レコードを設定するには、そのドメインとネーム サーバ上でホストされているドメインの権限ネーム サーバの IP アドレスを指定する NS の回答を設定する必要があります。詳細については、第 6 章「回答グループの権限ドメインの作成」セクションを参照してください。

DNS 構造

特定のドメインまたはマシンのデータを必要とするエンド ユーザは、クライアント上で、ローカルな NS（別名、*D プロキシ*）に最初に送信される再帰 DNS 要求を生成します。D プロキシは、要求されたドメインの IP アドレスをエンド ユーザに返します。

DNS 構造は、一般的なファイル システムと類似した階層ツリー構造に基づいています。この構造の基幹となるコンポーネントを次に示します。

- DNS リゾルバ — クライアント ネーム サーバにアクセスするクライアント。
- クライアント ネーム サーバ — 要求された Web サイトの検出を担当する DNS ソフトウェアを実行するサーバ。クライアント ネーム サーバはクライアント DNS プロキシ（D プロキシ）とも呼ばれています。
- ルート ネーム サーバ — DNS 階層のトップに配置されているサーバ。ルート ネーム サーバは、ホスト名のピリオド（.）の後にくる拡張部分すべてを検出する方法を把握しています。トップレベル ドメインは多数あります。

もっとも一般的なトップレベル ドメインには、.org、.edu、.net、.gov、.mil などが含まれています。世界中にある約 13 のルート サーバがすべてのインターネット要求を処理しています。

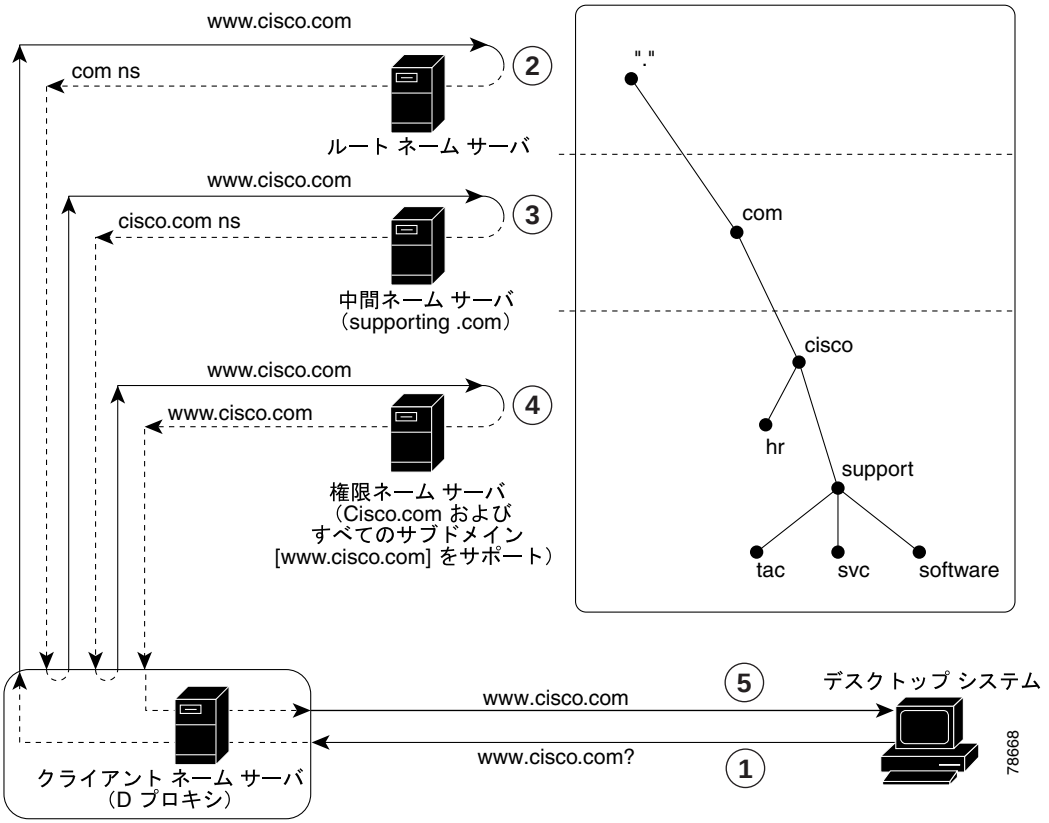
- 中間ネーム サーバ — 拡張目的で使用されるサーバ。ルート ネーム サーバが権限ネーム サーバの IP アドレスを持っていない場合、要求のクライアント ネーム サーバを中間ネーム サーバへ送信します。その後、中間ネーム サーバがクライアント ネーム サーバに権限ネーム サーバを参照させます。
- 権限ネーム サーバ — 要求されたドメインの権限を持つ企業に運営されているサーバ、またはサービス プロバイダーに外部委託されたサーバ。権限ネーム サーバは、要求された IP アドレスの（該当クライアントではなく）クライアント ネーム サーバに直接応答します。

要求解決

エンド ユーザから要求された情報がローカル D プロキシ内に存在しない場合、D プロキシは、要求されたドメイン付近のドメインについて信頼できると判断したネーム サーバに反復要求を送信します。たとえば、www.cisco.com に対する要求があると、D プロキシは最初に www.cisco.com について信頼できる別のネーム サーバがあるかを調べます。

図 1-2 に示されている概要プロセスは、クライアントが www.cisco.com の Web サイトにアクセスしようとする際に、IP アドレスを返すために DNS 構造が実行する順番を要約しています。

図 1-2　DNS 要求解決



1. リゾルバ（クライアント）が、www.cisco.com のクエリーをローカルのクライアント ネーム サーバ（D プロキシ）に送信します。
2. ローカルの D プロキシは www.cisco.com の IP アドレスを保有していないため、ルート ネーム サーバ（“.”）にこの IP アドレスを問い合わせるためにクエリーを送信します。ルート ネーム サーバは、次のいずれかの方法で要求に応答します。
   - D プロキシに .com ドメインをサポートしている特定のネーム サーバを照会します。
   - www.cisco.com の権限ネーム サーバのアドレスを把握している中間ネーム サーバに D プロキシを送信します。この方法は*反復クエリー*と呼ばれます。

3. ローカルの D プロキシは、cisco.com とそれに関連するすべてのサブドメインの権限ネーム サーバを照会されたあと、応答する中間ネーム サーバにクエリーを送信します。
4. ローカルの D プロキシは、トップレベル ドメインである cisco.com の権限ネーム サーバにクエリーを送信します。この例では、www.cisco.com は cisco.com のサブドメインです。このネーム サーバは要求されたドメインの権限を保有しているため、ネーム サーバ（D プロキシ）に IP アドレスを送信します。
5. ネーム サーバ（D プロキシ）は、クライアントに IP アドレス（172.16.56.76）を送信します。ブラウザはこの IP アドレスを使用して、www.cisco.com の Web サイトへ接続を開始します。

DNS 装置としての GSS

GSS は、DNS 要求に基づいて地理的に分散されたデータセンターの負荷を分散します。またそれ以外にも、送信元サーバやサードパーティ製の SLB のような、DNS システムに登録できる DNS 対応デバイスの負荷も分散します。負荷分散の詳細については、「GSS を使用したグローバル ロード バランシング」を参照してください。

通常、GSS は DNS 階層内のサブレベルで動作し、特定の DNS クエリーのサブセットに対してのみ応答します。そのため、ユーザは他の DNS クエリー タイプを処理する場合、DNS サーバを使用する必要があります。

v2.0 リリースでは、GSS の製品機能が拡張されたため、GSS を DNS 階層のトップレベルに移行させることが可能になりました。この拡張は、GSS を DNS デバイスのように動作することを許可する Cisco Network Registrar（CNR; Cisco ネットワーク レジストラ）と連動させることで実現しました。これにより、DNS 構造の管理と設定の処理を簡単にすることができます。

この 2 つの連動は、1 つの物理的なハードウェア上で稼働している別々のサブシステムとして確認できます。GSS はすべての DNS 要求を受信するフロントエンド DNS サーバとして機能しています。

各クエリーは、タイプによって次のように処理されます。

- A クエリー — GSS はこれらのクエリーを処理し、回答が見つかれば応答します。回答を見つけることができない場合、CNR サブシステムに回答を問い合わせます。問い合わせ後に、CNR の回答は D プロキシに転送されます。
- 他のすべてのクエリー — これらのクエリーは CNR サブシステムに転送されます。CNR サブシステムからの応答は D プロキシに転送されます。応答の Additional Section に *A* レコードが含まれている場合、GSS はその *A* レコードの負荷を分散するために、自身のクエリー処理を実行して Response の Additional Section を変更します。

GSS と CNR の相互作用について、また、CNR ライセンスの取得方法や GSS への CNR ライセンス導入方法など、CNR と GSS の詳細については、『*Global Site Selector Administration Guide*』を参照してください。

GSS を使用したグローバル ロード バランシング

GSS は、致命的な災害復旧に対応できるように、別々に設置されたデータセンターの負荷をグローバルに分散します。GSS は、グローバル ネットワークで導入され、地理的に分かれている次のシスコ製の SLB の負荷を調整します。

- Cisco Content Services Switch 11500、11000、11150
- Catalyst 6500 シリーズ スイッチに対応した Cisco Content Switching Module（CSM）
- Cisco LocalDirector
- Cisco IOS SLB
- ネットワーク プロキシミティに Director Response Protocol（DRP）エージェントを使用したシスコ製のルータ
- HTTP HEAD、Internet Message Control Protocol（ICMP; インターネット制御メッセージ プロトコル）、TCP 要求に対応したサーバ
- キャッシュ モジュールを搭載したシスコ製のルータ
- Cisco Cache Engine

GSS は、4000 以上の Virtual IP（VIP; バーチャル IP）アドレスをそれぞれサポートします。また、管理されたこれらの装置の信頼できる DNS サーバとして機能することにより、SLB の動作を調整します。

GSS が GSLB サービスを受け持つことになると、DNS プロセスが GSS に移行されます。DNS 設定は、「要求解決」セクションで説明されているものとプロセスは同じです。唯一異なる点は、NS レコードが各データセンターにある GSS を指していることです。GSS はどのデータセンターがクライアント トラフィックを受信するかを判断します。

GSS は、ドメインまたはサブドメインの権限ネーム サーバとして、DNS 要求応答時に次の追加要因を考慮します。

- アベイラビリティ — クエリーに応答できるオンラインサーバ
- プロキシミティ — もっとも迅速に応答したサーバ
- 負荷 — ドメイン内のサーバが処理するトラフィック負荷のタイプ
- 要求の送信元 — コンテンツを要求しているネーム サーバ（D プロキシ）
- 初期設定 — クエリーへの応答に使用する 1 番目、2 番目、3 番目の負荷分散アルゴリズム

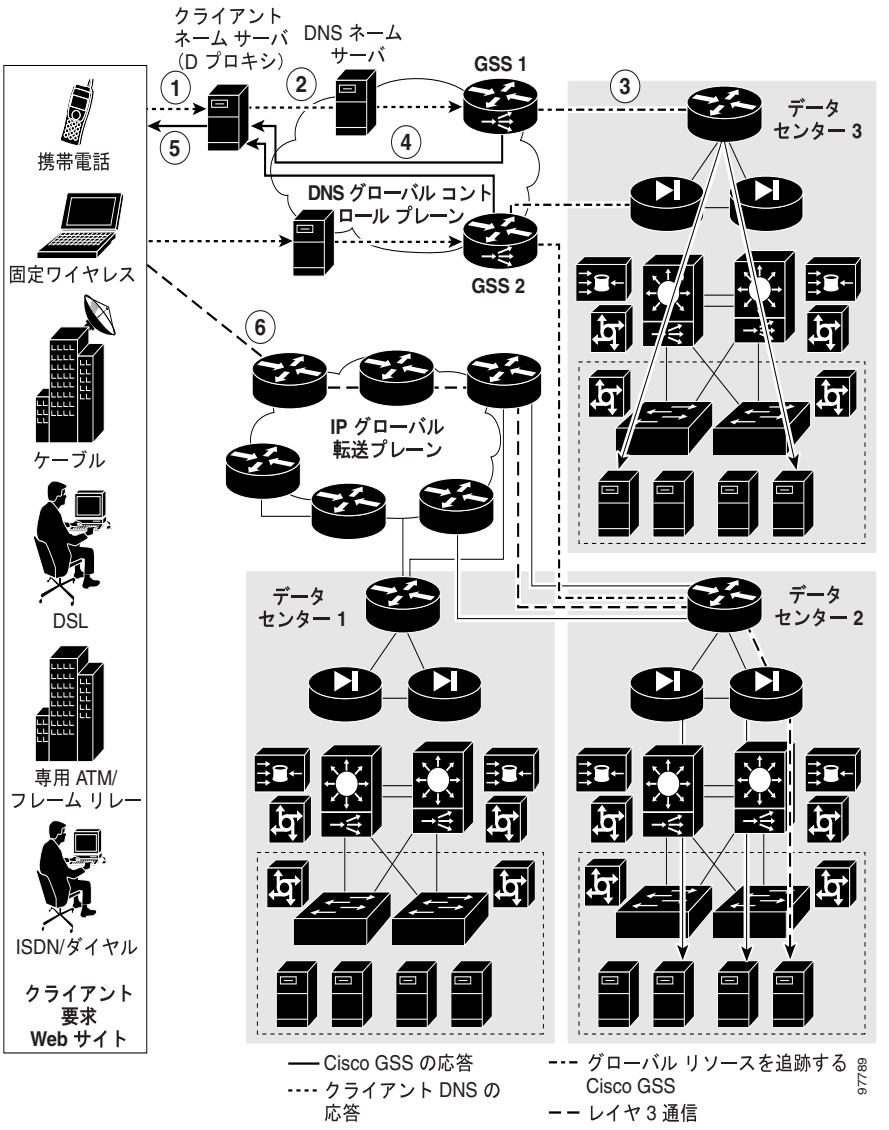
この GSLB タイプを使用すると、エンド ユーザが常にオンライン状態のリソースに転送されるとともに、要求が最適な装置に転送されるため、ユーザの応答時間が短縮されます。

GSS は DNS 要求の解決中に、管理されているリソースを考慮するための一連の各処理を実行して、要求元クライアントの D プロキシに最適な回答を戻します。

図 1-3 は、GSS が Web サイト選定プロセスの一部として、どのように各種クライアントと連携して要求されたコンテンツ サイトの IP アドレスを返すかを要約しています。

1. クライアントは www.cisco.com から最新バージョンのソフトウェア ダウンロードを開始するために、ブラウザの入力場所またはアドレス フィールドに **www.cisco.com** を入力します。このアプリケーションは 3 つの異なるデータセンターでサポートされています。
2. DNS のグローバル コントロール プレーン インフラストラクチャはその要求を処理したあと、GSS デバイスにその要求が到着します。
3. GSS はクライアントに「最適な」サーバ ロード バランサの IP アドレスを送信します（ここでは、データセンター 2 の SLB）。
4. Web ブラウザは送信された IP アドレスを処理します。
5. クライアントは IP コントロールと転送プレーンにより、データセンター 2 の SLB に誘導されます。
6. GSS は DNS グローバル コントロール プレーンのサイト選定プロセスの負荷を軽減します。要求とサイト選定は、ユーザが制御している負荷分散アルゴリズムの負荷情報と状態情報に基づいています。GSS は使用可能で負荷の低いデータセンターを即座に選択します。

図 1-3　Cisco Global Site Selector を使用した GLSB



GSS のアーキテクチャ

ここでは、ハードウェアやソフトウェアなど GSS 配置に関する主要コンポーネント、および GSS ネットワークの概念について説明します。主な内容は、次のとおりです。

- GSS および GSSM
- DNS 規則
- ロケーションおよびリージョン
- 所有者
- 送信元アドレスおよび送信元アドレス リスト
- ホステッド ドメインおよびドメイン リスト
- 回答および回答グループ
- キープアライブ
- 分散方法
- トラフィック管理の負荷分散

GSS および GSSM

プライマリ Global Site Selector Manager（GSSM）およびスタンバイ GSSM をはじめ、ネットワーク内のすべての GSS デバイスはドメインの権限を委任されており、DNS クエリーに応答し、キープアライブを実行します。また、ローカルで CLI（コマンドライン インターフェイス）を使用して、基本的なネットワーク管理も実行できます。中央集中型で共有の GSLB 機能を提供する場合、プライマリ GSSM によって、各 GSS デバイスは異なります。

ここでは、次の内容を説明します。

- プライマリ GSSM
- GSS
- スタンバイ GSSM

プライマリ GSSM

プライマリ GSSM は、GSS ソフトウェアを実行する GSS の 1 つです。この GSSM は、GSS ネットワークのコンテンツ ルーティングや中央集中型の管理、共有の GSLB 機能を実行します。

プライマリ GSSM は、すべての GSS リソースの設定情報（個々の GSS や DNS 規則など）を含んだあらかじめ搭載されている GSS データベースをサービスします。接続されたすべての GSS デバイスは自身のステータスをプライマリ GSSM に報告します。

プライマリ GSSM では、次の方法のいずれかを使用して、GSS デバイスの監視および管理を実行できます。

- GUI（グラフィカル ユーザ インターフェイス）機能
- CLI コマンド（『*Cisco Global Site Selector CLI-Based Global Server Load-Balancing Configuration Guide*』を参照）

変更した設定はすべて、プライマリ GSSM によって各デバイスに自動的に通信されます。

すべての GSS デバイスは、設定されたシステム上で単一のプライマリ GSSM としてサービスできます。

GSS

GSS は GSS ソフトウェアを実行し、プライマリ GSSM を使用して設定された DNS 規則と条件に基づいて DNS クエリーをルーティングします。

各 GSS はプライマリ GSSM に把握されており、同期をとられます。

各 GSS は CLI を使用して個別に管理します。GUI は GSS または スタンバイ GSSM 上ではサポートされていません。

スタンバイ GSSM

スタンバイ GSS は GSS ソフトウェアを実行する GSS の 1 つで、プライマリ GSSM を使用して設定された DNS 規則と条件に基づいて DNS クエリーをルーティングします。また、スタンバイ GSSM は、指定のプライマリ GSSM が突然オフラインになったり、他の GSS デバイスと通信不能になった場合に、プライマリ GSSM として機能するように設定されています。

スタンバイ GSSM には、一時的にプライマリ GSSM として動作する場合に備え、現在プライマリ GSSM にインストールされている組み込みの GSS データベースの重複コピーが含まれています。スタンバイ GSSM は一時的なプライマリ GSSM として設定されると、CLI および GUI の両方がサポートされます。プライマリ GSSM として動作している間は、GSS の動作を監視し、必要に応じて設定を変更できます

GSS ネットワークに影響するすべての設定またはネットワークの変更はプライマリ GSSM とスタンバイ GSSM 間で同期されるため、2 つのデバイスの動作は常に一致します。

スタンバイ GSSM をプライマリ GSSM として有効にするには、**gssm standby-to-primary** CLI コマンドを使用します。スタンバイ GSSM を新しいプライマリ GSSM として有効にする前に、元のプライマリ GSSM がオフラインになっていることを確認してください。

注意　2 つのプライマリ GSSM を同時にアクティブにすると、GSS ネットワークの構成変更が不意に削除されることがあります。このような二重のプライマリ GSSM 設定を発生させた場合、2 つのプライマリ GSSM がスタンバイ モードに戻ります。その後、どちらかの GSSM をプライマリ GSSM として再設定してください。

スタンバイ GSSM は、プライマリ GSSM が使用不能になった場合、一時的にプライマリ GSSM の役割を担うことができます（プライマリ GSSM を移動させる必要がある場合、または修復や保守のためにオフラインにする必要がある場合など）。指定のプライマリ GSSM とスタンバイ GSSM との役割の切り替えは、元のプライマリ GSSM がオンラインに戻るまでの一時的な GSS ネットワーク設定で

あることが想定されています。『*Cisco Global Site Selector Administration Guide*』に説明されているように、元のプライマリ GSSM が使用可能になれば、2 つとも GSS ネットワークでの元の役割が再度割り当てられます。

DNS 規則

プライマリ GSSM では、次のような DNS 規則を設定できます。

- 指定のホステッド ドメインで GSS が行うグローバルな負荷分散方法に関する中央集中型のコマンドと制御
- クライアント ネーム サーバ（D プロキシ）に送信するための IP アドレスの定義
- 使用する復旧方法の定義（最大 3 つの負荷 balance 句を使用）

各 DNS 規則は、既知の送信元または D プロキシから受信した要求を、ネームサーバまたは VIP のグループ内の最適なメンバーと照合して、受信した各クエリーへの応答方法を決定します。

各 DNS 規則は、次の変数を使用します。

- 要求元 D プロキシの送信元 IP アドレス
- 要求されたホステッド ドメイン
- 回答グループ（応答に必要とみなされているリソース グループ）
- 分散方法（最適なサーバ、分散方法、および句を構成する回答グループを選択するためのアルゴリズム）
- DNS スティッキやネットワーク プロキシミティのような詳細なトラフィック管理負荷分散機能

DNS 規則における GSS での要求の処理方法を定義するには、次の質問に回答してみてください。

> *いつ特定のドメイン名を問い合わせるトラフィックが DNS プロキシから着信したか？応答に関して考慮する必要があるリソースはどれか？ どのように負荷を分散させるべきか？*

各 GSS ネットワークは、最大 4000 の DNS 規則をサポートしています。

各 DNS 規則では、回答グループと balance 句を最大 3 つ応答に使用できます。各句は、特定の回答グループが要求を処理し、特定の分散方法を使用して回答グループから最適なリソースを選択するように指定します。これらの句は設定されたパラメータで順番に評価され、最初の回答グループと指定の分散方法が回答にたどり着かない場合に、いつスキップして次の句を使用するかを決定します。

GSS ネットワークですべてのグローバル サーバ ロード バランシングを管理する DNS 規則の構築方法については、第 7 章「DNS 規則の作成および変更」を参照してください。

ロケーションおよびリージョン

GSS ネットワークが拡大するにつれ、GSS リソース（ロケーション、リージョン、回答と回答グループ、ドメイン リスト、および DNS 規則）を編成および管理する作業がますます複雑になります。そのようなリソース編成を軽減するために、GSS は次の機能を提供しています。

- ロケーション — 都市、データセンター、コンテンツ サイトなど、地理的な範囲に対応する GSS リソースの論理グループ
- リージョン — 1 つまたは複数のロケーションを含む、より高度な地理的グループ

ロケーションやリージョンのような論理グループを使用すると、長い回答リスト、DNS 規則などを簡単に並べ替えたり、ナビゲートできるだけでなく、GSS リソースの一括管理を簡単に実行できます。たとえばプライマリ GSSM から、特定の GSS データセンターにリンクされたすべての回答を中断またはアクティブ化できます。マウスを数回クリックするだけで、スケジュールされている保守作業のためにサイトをシャットダウンし、その後、再びオンラインに戻すことができます。

ロケーションおよびリージョンの設定に関する詳細は、第 2 章「リソースの設定」を参照してください。

所有者

所有者は Web コンテンツを所有するエンティティで、GSS を使用してそのコンテンツのアクセスを管理します。ロケーションやリージョンを使用すると GSS ネットワークを地理的に設定できるように、所有者を使用すると GSS ネットワークを組織的に設定できます。

たとえば、GSS を使用して複数のホスティング サイトを管理するサービス プロバイダーは、ユーザをホスティングしている Web またはアプリケーションごとに所有者を作成することができます。この組織的な方式により、さまざまな要素（所有者のホストするコンテンツを含むドメイン リスト、DNS 規則、回答グループ、ドメインに対するトラフィック処理方法を指定する送信元アドレス リスト）を各所有者と関連付けて管理できます。

企業イントラネットに導入した場合、所有者を設定して GSS リソースを部門単位で分離したり、特定のリソースを IT 担当者に割り当てることができます。たとえば、会計、人事、および営業部門の所有者を作成して、それぞれに対応するリソースをまとめて表示したり、管理することができます。

所有者の設定に関する詳細は、第 2 章「リソースの設定」を参照してください。

送信元アドレスおよび送信元アドレス リスト

送信元アドレスという用語は、GSS で受信された DNS クエリーの送信元を表します。通常、送信元アドレスは、クエリーの送信元であるクライアントの D プロキシを表す IP アドレスまたはアドレス ブロックのことを意味します。

DNS 規則を使用することにより、GSS は複数の分散方法のいずれかを使用して、GSS でホスティングされるドメインと送信元アドレスを比較します。

送信元アドレスは、要求元クライアントが再帰要求を発行した D プロキシ（ローカル ネーム サーバ）から取得されます。D プロキシはクライアントのクエリーを複数のサーバに送信し、最終的に GSS に問い合わせ、設定済みの送信元アドレスのリストと D プロキシ の送信元アドレスを比較します。

GSS で受信された DNS クエリーをルーティングする場合は、このクエリーを特定の D プロキシと比較する必要はありません。既知の送信元アドレスから送られなかった要求には、デフォルト ルーティングを実行できます。デフォルトでは、GSS にフェールセーフの「Anywhere」送信元アドレス リストが用意されています。設定済み送信元アドレス リストと一致しない着信クエリーは、このリストと比較されます。

特定の IP アドレスの他に、プレフィクスが可変長の Classless Interdomain Routing（CIDR）ブロック マスキングを使用して、アドレス ブロックを表す送信元アドレスを設定することもできます。次に、受信可能な GSS の送信元アドレス例を示します。

```
192.168.1.110
192.168.1.110/32
192.168.1.0/24
192.168.0.0/16
```

送信元アドレスは、要求をルーティングするために、リスト（送信元アドレス リスト）にグループ化されます。送信元アドレス リストには 1 ～ 30 個の送信元アドレス、または一意のアドレス ブロックを格納できます。各 GSS は、最大 60 の送信元アドレス リストをサポートします。

送信元アドレス リストの設定に関する詳細は、第 3 章「送信元アドレス リストの作成」を参照してください。

ホステッド ドメインおよびドメイン リスト

HD（ホステッド ドメイン）は、GSS に委任され、プライマリ GSSM の GUI を使用して DNS クエリー応答用に設定された任意のドメインまたはサブドメインです。ホステッド ドメインは GSS が信頼している DNS ドメイン名です。

すべての DNS クエリーは、設定されたドメイン リスト内のドメインに一致する必要があります。一致しない DNS クエリーは、GSS によって拒否されます。GSS ドメイン リストのドメインと一致しないクエリーは、GSS によって外部 DNS ネーム サーバに転送して解決することもできます。

ホステッド ドメインは最大 128 文字です。GSS はワイルドカードを使用したドメイン名をサポートしています。また、ワイルドカードを比較させるときの正規表現として、Portable Operating System Interface for UNIX（POSIX）1003.2 拡張正規表現もサポートしています。

GSS では次のドメインまたはサブドメイン名を設定できます。

```
cisco.com
www.cisco.com
www.support.cisco.com
.*\.cisco\.com
```

ドメイン リストは GSS に委任されたホステッド ドメインのグループです。各 GSS は、最大 2000 のホステッド ドメインと、2000 のホステッド ドメイン リストをサポートしています。また、各ドメイン リストは、最大 500 のホステッド ドメインをサポートしています。

GSS はドメイン リストを使用して、着信する DNS 要求と DNS 規則を照合します。クエリーのドメインがドメイン リスト内で検出され、DNS 規則と照合されたあと、DNS 規則の balance 句によって、その要求をサービスできる最適な回答（VIP など）を GSS がどのように選定するかが定義されます。

ドメイン リストの設定に関する詳細は、第 4 章「ドメイン リストの設定」を参照してください。

回答および回答グループ

GSS ネットワークでは、回答という用語は、受信する DNS 要求を GSS が解決するリソースを表します。GSS ネットワークでは、次の 3 つのタイプの回答が可能です。

- VIP — CSS、CSM、Cisco IOS に準拠した SLB、LocalDirector、Web サーバ キャッシュ、グローバル ネットワークの配置で地理的に分散している他の SLB など、SLB に関連付けられた VIP アドレス。
- ネーム サーバ — 設定された DNS ネーム サーバで、GSS が解決できないクエリーを回答できます。

（注） GSS がスタンドアロン モードに設定されている場合、GSS が DNS 解決を正常に実行できるようにネーム サーバを適切に設定し、確実に稼働させる必要があります。CNR が v2.0 の GSS にインストールされている場合、ネーム サーバは不要です。

- CRA — Content Routing Agent（CRA; コンテンツ ルーティング エージェント）は、DNS レースと呼ばれる解決処理を使用して、同一の応答を同時にユーザの D プロキシに戻します。

ドメインおよび送信元アドレスと同様に、回答はプライマリ GSSM の GUI を使用して設定されます。そのためには、クエリーを転送できる IP アドレスを指定する必要があります。

回答は一度作成されると、回答グループと呼ばれるリソース プールにグループとしてまとめられます。GSS は、使用できる回答グループから可能性のある応答として最大 3 つの回答グループと、DNS 規則の balance 句を使用して、ユーザの要求をサービスするためにもっとも適したリソースを選択できます。各 balance 句は、設定された回答グループから 1 つの回答を選択するのに別々のアルゴリズムを提供します。各句は、特定の回答グループが要求を処理し、特定の分散方法を使用して回答グループから最適なリソースを選択するように指定します。

回答タイプに応じて、DNS クエリーに追加の規則を適用して、最適なホストを選択することができます。たとえば、Cisco CSS に関連づけられた VIP にルーティングされる要求は、CSS で判別された負荷およびアベイラビリティに基づいて、最適なリソースにルーティングされます。CRA にルーティングされる要求は、GSS によって実行される DNS レースで判別されたプロキシミティに基づいて、最適なリソースにルーティングされます。

GSS の回答および回答グループの設定に関する詳細は、第 6 章「回答および回答グループの設定」を参照してください。

ここでは、次の内容を説明します。

- VIP 回答
- ネーム サーバ回答
- CRA 回答

VIP 回答

SLB は VIP 回答を使用して、自身が制御する 1 つ以上のサーバでホストされているコンテンツを示します。VIP 回答を使用することで、GSS は複数の送信元サーバ、アプリケーション サーバ、またはトランザクション サーバ間でトラフィックを分散して、ユーザの応答時間を短縮し、ホストのネットワーク輻輳を軽減することができます。

VIP 回答タイプに関連づけられたドメインに対してクライアントの D プロキシから問い合わせがあった場合、GSS はその要求を処理するために最適な SLB の VIP アドレスを使用して応答します。次に、要求元クライアントが SLB に問い合わせを行い、そこで応答に最適なサーバに要求を負荷分散します。

ネーム サーバ回答

ネーム サーバは、GSS から送信された DNS クエリーの転送先となる DNS ネーム サーバの IP アドレスを指定します。

クエリーは、ネーム サーバの転送機能を使用して、外部（GSS 以外の）ネーム サーバに転送されて解決されます。回答は GSS ネーム サーバに戻され、そこから要求元の D プロキシに戻されます。ネーム サーバ回答は信頼できるフォールバック リソースとして動作可能で、GSS が解決できない要求の解決に使用されます。GSS が要求を解決できない場合、次の理由が挙げられます。

- 要求されたコンテンツが GSS に不明な場合
- 通常、取り扱いできない要求として処理されるリソースの場合

GSS によって転送された外部 DNS ネーム サーバ回答は、次の機能を実行できる場合があります。

- Mail Exchanger（タイプ MX）レコードのような、GSS にサポートされていない DNS サーバ機能を使用
- フェールオーバーとエラー回復のためのサードパーティのコンテンツ　プロバイダーを使用
- 段階的に DNS システムへのアクセスを提供

CRA 回答

CRA 回答は、CRA および GSS を信頼し、複数の可能なホストと要求元 D プロキシとの距離に基づいて、指定されたクエリーに最適な回答を選択します。

CRA 回答が指定されている場合、特定の D プロキシから受信した要求は、最初に要求に応答するコンテンツ サーバによって処理されます。応答時間は DNS レースを使用して測定され、GSS および各コンテンツ サーバで稼働している CRA によって調整されます。DNS レースでは、複数のホストが A レコードの要求に同時に応答します。応答時間が最短のサーバ（サーバ自身と D プロキシ間のネットワーク遅延が最短のサーバ）が、コンテンツ処理用に選択されます。

DNS レースを開始する前に、GSS には次の情報が必要です。

- GSS と各データセンター内の各 CRA の間の遅延。このデータを使用して、GSS は各データセンターからのレースの遅延を計算し、各 CRA がレースを同時に開始できるようにします。
- キープアライブを使用した CRA のオンライン状況。

ブーメラン分散方法では、DNS レースを使用して、最適なサイトを判別します。この分散方法の詳細については、「DNS レース（ブーメラン）方法」セクションを参照してください。

キープアライブ

リソースを指定するだけでなく、各回答にはリソースのキープアライブを指定するオプションも用意されています。キープアライブは、リソースが依然として有効であるかどうかを確認するために、GSS が定期的にチェックする方式です。キープアライブは、共通にサポートされたプロトコルを使用して GSS と他のデバイス間で行う特別な相互動作です。キープアライブは、デバイス上の特定のプロトコルが適切に機能するかどうかテストするように設計されています。ハンドシェイクが成功すると、デバイスが使用可能になります。次にアクティブになり、最後にトラフィックを受信できるようになります。ハンドシェイクが失敗すると、デバイスは使用不可で動作していないとみなされます。すべての回答は設定済みのキープアライブによって検証され、回答が使用不可能であることをキープアライブが示している場合、GSS から D プロキシへの回答は戻されません。

GSS はキープアライブを使用して、VIP のオンライン ステータスから、サーバ上で稼働しているサービスおよびアプリケーションにいたるまで、すべての情報を収集および追跡します。キープアライブを設定することで、リソースのオンライン状況を継続的に監視し、その情報をプライマリ GSSM に報告できます。対象のリソースのルーティングの判断には、その報告されたオンライン状況も含まれます。

GSS は、監視対象の GSS と SLB 間のトラフィックを軽減するために、共有キープアライブの使用もサポートしています。共有キープアライブは、複数の回答状況を伝えることができる共通の IP アドレスまたはリソースを識別します。共有キープアライブはネーム サーバ または CRA 回答と一緒には使用されません。

VIP タイプの回答を作成する場合、さまざまなキープアライブ タイプまたは複数のキープアライブ タイプの 1 つを設定して、目的の回答をテストできます。プライマリ GSSM は、特定の VIP 回答に対して複数のキープアライブと宛先ポートの割り当てをサポートします。ICMP、TCP、HTTP HEAD、KAL-AP VIP キープアライブ タイプの混在や比較設定で、1 つの VIP 回答に対し、最大 5 つの異なるキープアライブを設定できます。TCP または HTTP HEAD キープアライブの場合、VIP サーバに異なる宛先ポートも指定できます。

次のセクションでは、GSS でサポートされる各種キープアライブ タイプを説明します。

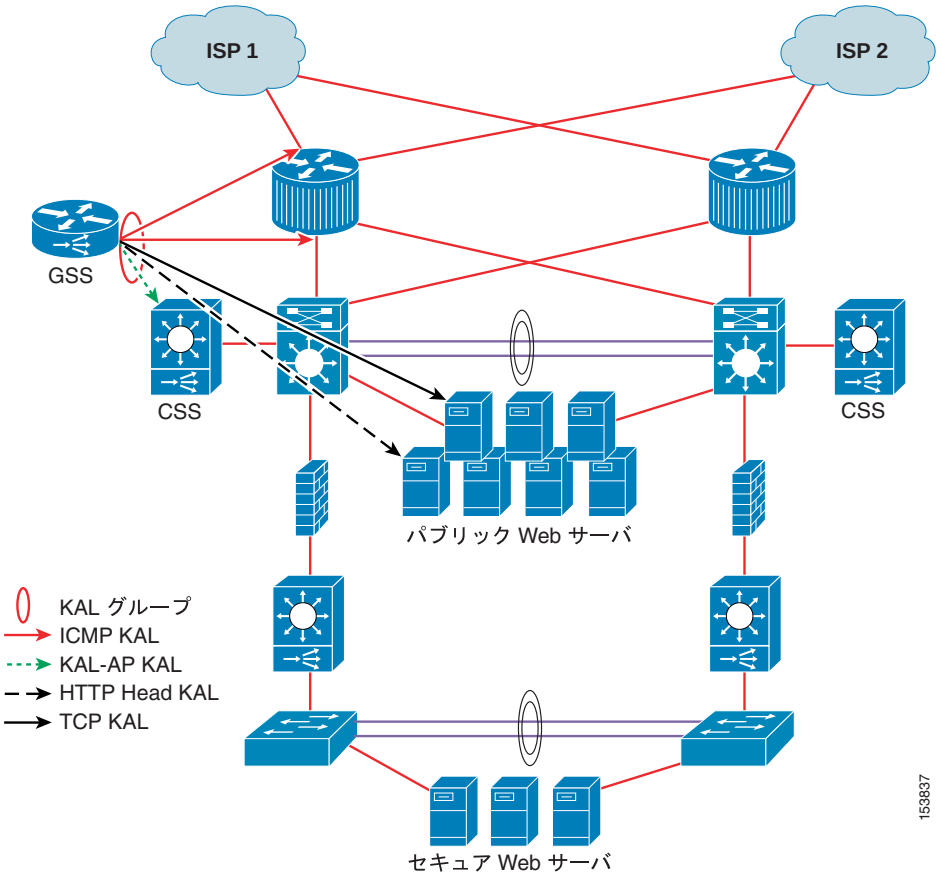
- ICMP
- TCP
- HTTP-HEAD
- KAL-AP
- Scripted キープアライブ
- ネーム サーバ
- None
- キープアライブの障害検出時間の調整

マルチポート キープアライブ

GSS は、VIP タイプの回答でマルチポート キープアライブを使用して、複数のデバイスの監視をサポートします。VIP サーバの複数のポートを監視するために、異なるタイプのキープアライブを設定できます。また、VIP サーバ以外の IP アドレスを指定するキープアライブも設定できます (ルータ、バックエンド データベース サーバ、Catalyst 6500 シリーズ スイッチ、データセンター構成の CSS など)。

グループとして機能し、かつ特定のデバイスをプローブするよう設定された各キープアライブが、対象の設定のオンライン状況を監視します。すべてのキープアライブが成功するかぎり、GSS デバイスは設定が有効であるとみなし、トラフィックをデータセンターに送信し続けます。データセンターで複数のデバイスをプローブするキープアライブの設定例は、図 1-4 を参照してください。

図 1-4　複数のキープアライブを使用してデータセンターを監視



（注）　プライマリ GSSM を使用すると、複数のキープアライブ タイプの設定時に、単一の KeepAlive-Appliance Protocol（KAL-AP）キープアライブだけでなく、複数の共有キープアライブを設定できます。

グローバル キープアライブ パラメータの変更と共有キープアライブの作成については、第 5 章「キープアライブの設定」を参照してください。

ICMP

VIP アドレス、IP アドレス、または仮想サーバの IP アドレスの GSS 回答をテストする場合、ICMP キープアライブを使用します。ICMP キープアライブ タイプは、回答に対して、設定された VIP アドレス（または共有キープアライブ アドレス）への ICMP パケットを含むクエリーを発行して、リソースの状態を監視します。オンライン状況（ネットワークに単に接続されているかどうか）は、対象アドレスからの応答によって判別されます。GSS では、標準の検出方法を使用した場合、最大 750 の ICMP キープアライブがサポートされます。また、高速な検出方法を使用した場合、最大 150 の ICMP キープアライブがサポートされます。詳細については、「キープアライブの障害検出時間の調整」を参照してください。

TCP

CSS または CSM 以外の GSLB デバイスである GSS 回答をテストする場合、TCP キープアライブを使用します。GSLB リモート デバイスには、Web サーバ、LocalDirectors、Wireless Application Protocol（WAP）ゲートウェイ、TCP キープアライブを使用して確認可能な他のデバイスが含まれます。TCP キープアライブは、スリーウェイ ハンドシェイク シーケンスを使用して、リモート デバイスに TCP 接続を開始します。

TCP 接続が確立されると、GSS は接続を切断します。接続の終了方法として Reset（ハード リセットを使用した迅速な切断）または Graceful（標準のスリーウェイ ハンドシェイクを使用した切断）の方法を選択できます。

GSS では、標準の検出方法を使用した場合、最大 1500 の TCP キープアライブがサポートされます。また、高速な検出方法を使用した場合、最大 150 の TCP キープアライブがサポートされます。詳細については、「キープアライブの障害検出時間の調整」を参照してください。

HTTP-HEAD

スタンドアロン デバイスとして機能している HTTP Web サーバの GSS 回答、または Cisco CSS、Cisco CSM、Cisco IOS 準拠の SLB、Cisco LocalDirector などの SLB デバイスに管理されている HTTP Web サーバの GSS 回答をテストする場合、HTTP HEAD キープアライブを使用します。HTTP HEAD キープアライブ タイプは、指定のアドレスの Web サーバに TCP 形式の HTTP HEAD 要求を送信します。デバイスのオンライン状況は、HTTP Response Status Code（応答ステータス コード）200 からも判断されます（例：HTTP/1.0 200 OK）。

HTTP HEAD 接続が確立されると、GSS は接続を切断します。接続の終了方法には、Reset（ハード リセットを使用した迅速な切断）または Graceful（標準のスリーウェイ ハンドシェイクを使用した切断）の 2 つの方法があります。

GSS では、標準の検出方法を使用した場合、最大 500 の HTTP HEAD キープアライブがサポートされます。また、高速な検出方法を使用した場合、最大 100 の HTTP HEAD キープアライブがサポートされます。詳細については、「キープアライブの障害検出時間の調整」セクションを参照してください。

KAL-AP

Cisco CSS または Cisco CSM に関連付けられた VIP の GSS 回答をテストする場合、KeepAlive-Appliance　Protocol（KAL-AP）キープアライブを使用します。KAL-AP キープアライブ タイプは、指定のプライマリ（マスター）とオプションのセカンダリ（バックアップ）回線アドレスの両方に詳細なクエリーを送信します。送信後、KAL-AP キープアライブに指定された各 VIP のオンライン状態と負荷が戻ります。

GSS ネットワークの設定に応じた KAL-AP キープアライブを使用して、VIP アドレスに直接問い合わせをしたり（KAL-AP By VIP）、英数字のタグを持ったアドレスを問い合わせ（KAL-AP By Tag）したりできます。KAL-AP By Tag キープアライブ クエリーを使用すると、次のようなときに役立ちます。

- Network Address Translation（NAT; ネットワーク アドレス変換）を実行中のファイアウォールの後ろにあるデバイスのオンライン状況を判断しようとしている場合
- SLB に複数のコンテンツ規則の選択がある場合

GSS では、標準の検出方法を使用した場合、最大 128 のプライマリ KAL-AP と 128 のセカンダリ KAL-AP キープアライブがサポートされます。また、高速な検出方法を使用した場合、最大 40 の プライマリ KAL-AP と 128 のセカンダリ KAL-AP キープアライブがサポートされます。詳細については、「キープアライブの障害検出時間の調整」セクションを参照してください。

Scripted キープアライブ

サードパーティ製のデバイスをプローブして負荷情報を取得する場合、Scripted キープアライブを使用します。Scripted キープアライブは、SNMP（簡易ネットワーク管理プロトコル）Get 要求を使用して、目的のデバイスから負荷情報を取得します。

（注）　Scripted キープアライブは、常に共有キープアライブである必要があります。

GSS では、標準の検出方法を使用した場合、最大 384 の Scripted キープアライブがサポートされます。また、高速な検出方法を使用した場合、最大 120 の Scripted キープアライブがサポートされます。詳細については、「キープアライブの障害検出時間の調整」セクションを参照してください。セカンダリの Scripted キープアライブは GSS ではサポートされていません。

CRA

DNS レース要求に応答する CRA 回答をテストする場合、CRA キープアライブを使用します。CRA キープアライブ タイプは、情報パケットが CRA に到達して GSS に戻ってくるために必要な時間（ミリ秒）を追跡します。GSS は、最大 200 の CRA キープアライブをサポートします。

ネーム サーバ

指定のクエリー ドメイン（例 ; www.cisco.com）のネーム サーバの IP アドレスへクエリーを送信する場合、ネーム サーバ キープアライブを使用します。ネーム サーバ回答のオンライン状態は、クエリーへの応答、およびアドレスに対するドメイン割当てを実行するクエリー ドメインのネーム サーバの機能によって決まります。GSS は、最大 100 の ネーム サーバ キープアライブをサポートします。

None

キープアライブが None に設定されている場合、GSS は名前指定された回答が常にオンラインであると想定します。キープアライブ タイプを None に設定すると、GSS はルーティング時にオンライン ステータスまたは負荷を考慮しなくなります。ただし、他のキープアライブ タイプに適さない GSS ネットワークに装置を追加する場合など、特定の状況では、このタイプが役に立ちます。ICMP はほとんどの装置で使用できる単純で柔軟なキープアライブ タイプです。None オプションを使用するよりも、ICMP を使用することを推奨します。

キープアライブの障害検出時間の調整

GSS の障害検出時間は、デバイスに障害が発生してから（回答リソースがオフラインになる）、GSS がその発生した障害を認識するまでの総時間です。応答パケットがこの時間内に GSS に戻らない場合、回答がオフラインにマークされます。

GSS は、標準と高速の 2 つの検出モードをサポートしています。

標準モードを使用すると、GSS が生涯発生を検出するまでの障害検出時間は、通常 60 秒です。標準モードを使用すると、次のパラメータを調整できます。

- Response Timeout — 要求に応答していないデバイスに GSS がデータを再送信する前の許容時間。有効な入力値は 20 ～ 60 秒です。デフォルト値は 20 に指定されています。
- Minimum Interval — GSS がキープアライブのスケジューリングに使用する最低間隔。有効な入力値は 40 ～ 255 秒です。デフォルト値は 40 に指定されています。

高速モードの場合、GSS は次のキープアライブ転送間隔の数式を使用して、障害検出時間を制御します。

(*# Ack'd Packets* * [*Response TO* + [*Retry TO* * *# of Retries*]]) + *Timed Wait*

数式の各要素は次のとおりです。

 # Ack'd Packets = 確認回答形式が必要なパケット数

Response TO = Response Timeout（応答タイムアウト）。確認回答が必要なパケットの応答待機時間

Retry TO = Retry Timeout（再試行タイムアウト）。再送信されたパケットに対する応答待機時間

# of Retries = Number of Retries（再試行回数）。デバイスがオフラインと決定される前に、GSS が障害発生中と思われるデバイスにパケットを再送信する回数。

Timed Wait = 終了するためのリモート側の接続時間（TCP ベースのキープアライブ専用）

表 1-1 に、回答ごとの単一のキープアライブに対する GSS の高速キープアライブ転送率の算出方法をまとめます。

表 1-1　回答ごとの単一のキープアライブに対するキープアライブ転送率

	# Ack'd Packets（固定値）	Response TO（固定値）	Retry TO（固定値）	# of Retries（ユーザ選択）	Timed Wait（固定値）	転送間隔
KAL-AP	1	2 秒	2 秒	1	0	4 秒
ICMP	1	2 秒	2 秒	1	0	4 秒
TCP（RST）	1	2 秒	2 秒	1	0	4 秒
TCP（FIN）	2	2 秒	1 秒	1	2 秒	10 秒
HTTP HEAD（RST）	2	2 秒	2 秒	1	0	8 秒
HTTP HEAD（FIN）	3	2 秒	2 秒	1	2 秒	14 秒

TCP（RST）接続の場合、TCP キープアライブのデフォルトの転送間隔は、次のとおりです。

(1 * [2 + [2 * 1]]) + 0 = 4 秒

ICMP、TCP、HTTP HEAD、KAL-AP キープアライブ タイプの試行回数は調整できます。試行回数には、デバイスがオフラインと決定される前に、GSS が障害発生中と思われるデバイスにパケットを再送信する回数を定義します。GSS は、最大 10 回の再試行回数をサポートします（デフォルトは 1 回）。再試行回数を調節することは、GSS の検出時間を変更することと同じです。再試行回数を多く指定すれば、検出時間が長くなります。逆に、再試行回数を少なくすれば、検出時間は短くなります。

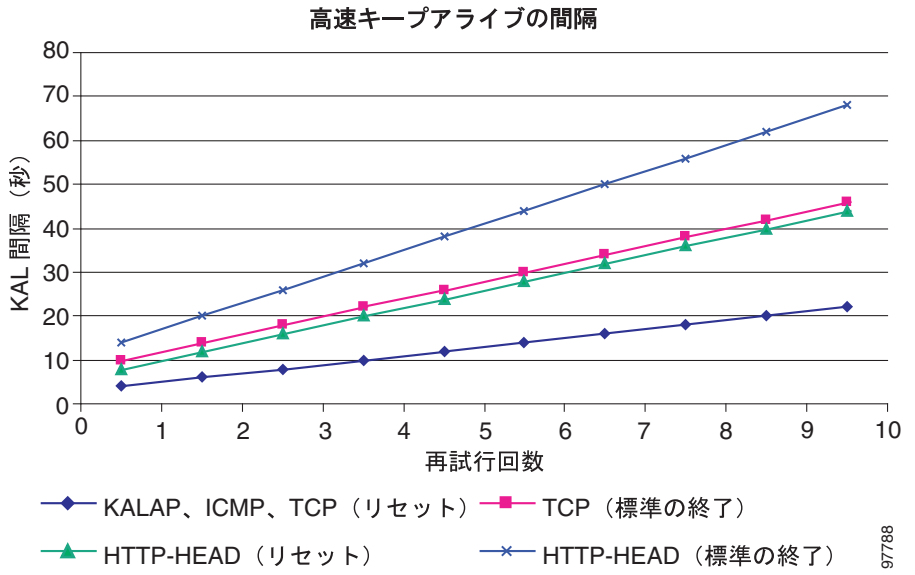
GSS は、キープアライブ サイクル（ICMP 要求、TCP SYN、TCP FIN）を継続する前に、再試行回数の値と、確認回答形式が必要な各パケットを関連付けます。たとえば、TCP ベースのキープアライブ サイクルを完全に実行する場合、TCP ベースのキープアライブは、指定の再試行回数分 SYN パケットを再試行したあと、指定の再試行回数分 FIN パケットを再試行することになります。

上記の TCP（RST）接続を例にとると、再試行回数のデフォルト値である 1 を 5 に変更した場合、転送間隔は次のようになります。

(1 * [2 + [2 * 5]]) + 0 = 12 秒

図 1-5 に、再試行回数の値を増やした場合のキープアライブ転送間隔の影響を示します。

図 1-5　キープアライブ転送間隔における再試行回数の値の影響



また、GSS がオフライン回答をオンラインと識別するときの判断材料になる、連続して成功したキープアライブ数（プローブ）も定義できます。GSS は、各キープアライブの試行回数を監視して、それが成功したかどうかを判断します。

Number of Successful Probes パラメータは、オンラインであるという回答を戻して GSS ネットワークに再導入する前に、GSS が認識する必要があるキープアライブの連続成功数です。

プライマリ GSSM は、1 つの VIP 回答に対して複数のキープアライブを割り当てることができます。ICMP、TCP、HTTP HEAD、KAL-AP VIP キープアライブ タイプの混在や比較設定で、1 つの VIP 回答に対し、最大 5 つの異なるキープアライブを設定できます。この設定にすると、障害検出時間は回答に関連付けられたそれぞれのキープアライブの算出された転送レベルに基づきます。

分散方法

GSS は 6 つの独自の分散方法をサポートしており、所定の DNS クエリーに応答する GSS 回答の選択方法を指定することができます。各 balance 句は、設定された回答グループから 1 つの回答を選択するのに別々のアルゴリズムを提供します。ここでは、GSS にサポートされている分散方法を説明します。

- 順序付きリスト方法
- ラウンドロビン方法
- 重み付けラウンドロビン方法
- 最小負荷方法
- ハッシュ方法
- DNS レース（ブーメラン）方法

順序付きリスト方法

GSS が順序付きリスト分散方法を使用すると、回答グループ内の各リソース（SLB VIP やネーム サーバなど）にグループ内の回答のランクに対応する番号が割り当てられます。割り当てられた番号は、リスト内の回答の順序を表します。リスト内の以降の VIP やネーム サーバは、リスト内のその前の VIP やネーム サーバが使用不可能な場合に限って使用されます。GSS では、順序付きリストに割り当てる番号が連続していなくてもかまいません。

（注）　回答グループ内で同じ順番を持つ回答がある場合、GSS はその番号を含む最初の回答のみ使用します。回答グループの各回答には、一意の順番を指定してください。

GSS は各回答にランキングを使用しており、各リソースを割り当てられた順序に並べ替えようとします。次に、ユーザ要求をサービスできる有効な回答を最初に選択します。リストのメンバーには所定の優先順位が設定されており、順序に従って実行されます。また、メンバーが使用されるのは、その前のすべてのメンバーで最適の結果が得られなかった場合に限ります。

順序付きリストの方法を使用すると、回答を選択するための決定論的方法が必要な複数のコンテンツ サイト間でリソースを管理できます。

順序付きリスト分散方法の使用時における、GSS の回答の選定方法については、「回答グループの分散方法オプション」セクションを参照してください。

ラウンドロビン方法

GSS がラウンドロビン分散方法を使用した場合、回答グループ内の各リソースは順番に実行されます。GSS は回答リスト内を循環し、各要求に対して次の回答を最初から順番に選択します。この方法では、GSS は使用可能な回答間で負荷を均等に分散して、要求を解決できます。

ラウンドロビン分散方法は、同一コンテンツをホスティングしている複数のアクティブなデータセンター間（プライマリ サイトの SLB と、要求を処理する「アクティブ スタンバイ」サイトの SLB 間など）で要求を分散する場合に便利です。

ラウンドロビン分散方法の使用時における、GSS の回答の選定方法については、「回答グループの分散方法オプション」セクションを参照してください。

重み付けラウンドロビン方法

ラウンドロビン分散方法と同様に、Weighted Round-Robin（WRR; 重み付けラウンドロビン）方法も、定義済みの回答リスト内を循環して、使用可能な各回答をそれぞれ順に選択します。ただし、WRR の場合は、各回答にさらに重み因子が割り当てられるため、特定のサーバに対する GSS が優遇されてその使用頻度が高まります。

重み付けラウンドロビン分散方法の使用時における、GSS の回答の選定方法については、「回答グループの分散方法オプション」セクションを参照してください。

最小負荷方法

最小負荷分散方法を使用すると、GSS はすべてのリソースの中で負荷が最小のリソースに対して要求を解決します。負荷が最小のリソースは、SLB の負荷およびアベイラビリティに関する詳細情報を GSS に提供する KAL-AP キープアライブ プロセスの報告に基づいて判別されます。

最小負荷分散方法は、CSM または最小負の CSS の最小接続数を判別することで要求を解決します。

最小負荷分散方法の使用時に、選択する回答を GSS が判別する方法については、「回答グループの分散方法オプション」セクションを参照してください。

ハッシュ方法

GSS がハッシュ分散方法を使用すると、クライアントの DNS プロキシの IP アドレスと要求元クライアントのドメインの要素が抽出され、ハッシュ値と呼ばれる一意の値が作成されます。一意のハッシュ値は、DNS クエリーの処理用に選択される VIP を識別するために付加したり、使用します。

ハッシュ値を使用すると、特定の要求元クライアントからのトラフィックを特定の VIP に「固定」して、今後そのクライアントから送信される要求を同一 VIP にルーティングすることができます。このタイプの方法は、クライアントからサイトへの接続が終了または中断した場合でもクライアント固有のデータが保持される、オンライン ショッピング バスケットなどの機能に適しています。

GSS は、次の 2 つのハッシュ分散方法をサポートします。指定の回答グループに対して、1 つまたは両方のハッシュ分散方法を適用できます。

- By Source Address — GSS は、要求の送信元アドレスから作成されたハッシュ値に基づいて回答を選択します。
- By Domain Name — GSS は、要求されたドメイン名から作成されたハッシュ値に基づいて回答を選択します。

DNS レース（ブーメラン）方法

GSS は近接ルーティングを使用した DNS レース（ブーメラン）方法をサポートします。これは、GSS によって開始される DNS 解決タイプで、2 ～ 20 のサイト間で負荷を分散します。

ブーメラン方法は、各データセンター内の CRA が A レコード（IP アドレス）を同時にクライアントの D プロキシに送信する場合、その瞬間のプロキシミティを判別できるという概念に基づいています。DNS レース方法による DNS 解決を使用すると、すべての CRA（シスコ コンテンツ エンジンまたはコンテンツ サービス スイッチ）にクライアントの要求を解決する機会が与えられるため、クライアントの D プロキシを証明せずにプロキシミティを判別できます。D プロキシで受信された最初の A レコードは、デフォルトで、もっとも距離が近いとみなされます。

GSS が DNS レースを開始するためには、CRA ごとに 次の情報を確立する必要があります。

- GSS と各データセンター内の各 CRA の間の遅延。このデータを使用して、GSS は各データセンターからのレースの遅延時間を計算し、各 CRA がレースを同時に開始できるようにします。
- CRA のオンライン状況。このデータを使用して、GSS は応答していない CRA に要求を転送しないようにします。

GSS のブーメラン サーバはあらかじめ定義された間隔でキープアライブ メッセージを送信して、この情報を収集します。ブーメラン サーバは、CRA の IP アドレスと一緒にこのデータとを使用して、DNS レースの正確な開始時刻を要求します。

D プロキシが CRA 応答を受け入れるためには、各 CRA は DNS 要求の送信元の GSS の IP アドレスをスプーフィングする必要があります。

回答グループの分散方法オプション

GSS にもっとも多くサポートされている分散方法で、回答グループの特定の回答をグループ化する場合、追加の設定オプションがあります。これらの設定オプションを使用すると、GSS は回答に適切な分散方法を確実に適用できます。つまり、GSS デバイスから最適な結果を得ることができます。

表 1-2 に、各回答タイプ（VIP、CRA、NS）と分散方法の組み合わせで使用可能な回答グループのオプションを示します。

表 1-2　回答グループ オプション

回答タイプ	使用する分散方法	回答グループ オプション
VIP	ハッシュ	Order
	最小負荷	LT（負荷スレッシュホールド）
	順序付きリスト	Weight
	ラウンドロビン	
	WRR	
ネーム サーバ	ハッシュ	Order
	順序付きリスト	Weight
	ラウンドロビン	
	WRR	
CRA	ブーメラン（DNS レース）	None

ここでは、回答グループの回答に使用できる各オプションを説明します。ここでの内容は、次のとおりです。

- Order
- Weight
- Load Threshold

Order

Order オプションは、回答グループの分散方法が順序付きリストの場合に使用します。要求に応答する場合は、リスト内の回答の位置に基づいて、リストの回答に優先順位が設定されます。

Weight

Weight オプションは、回答グループの分散方法が重み付けラウンドロビンまたは最小負荷の場合に使用します。重みは 1 ～ 10 の値を入力して指定します。この値は要求に応答する回答の容量を示します。重みによって、GSS が各回答に要求を送信するときの比率を作成します。たとえば、回答 A の重みが 10、回答 B の重みが 1 の場合、回答 B に要求が 1 つ転送されるたびに、回答 A は 10 個の要求を受信します。

WRR 分散方法に対して重みを指定する場合、GSS はリスト内の次の回答へ移る前に、要求への応答に使用する回答数の比率を作成します。

最小負荷分散方法に重みを指定する場合、GSS はその回答に関連した負荷数の計算時に、除数として値を使用します。この負荷数は、より大きな容量を持つ回答を優先させるバイアスを作成します。

Load Threshold

回答タイプが VIP、キープアライブ方法が KAL-AP の場合は、使用される分散方法に関係なく、使用可能な回答を判別できます。負荷スレッシュホールドは、回答デバイスから報告される負荷と比較する *n* 2 ～ 254 の数値です。報告された負荷が指定のスレッシュホールドを超えている場合、回答はオフラインであるとみなされ、これ以上要求を処理できなくなります。

トラフィック管理の負荷分散

GSS には、DNS スティッキとネットワーク プロキシミティ トラフィック管理機能が用意されており、GSS ネットワーク内で高性能なグローバル サーバ ロード バランシングを実行できます。

DNS スティッキを使用すると、カスタマーと e- コマース サーバ間で固定のスティッキ ネットワーク接続がサポートされるため、e- コマース サイトのサービスを中断させずに確実にビジネスを継続できます。固定のネットワーク接続により有効な接続が維持されるため、購入処理が完了する前にショッピング カードが紛失することもありません。

ネットワーク プロキシミティにより、要求元クライアントの D プロキシのロケーションまでの往復時間の測定に基づいて、もっとも近い（もっとも近接な）サーバが選択されます。これにより、GSS ネットワーク内の効率性が向上します。通常、ネットワーク トポロジが一定であれば、指定のロケーション（D プロキシ）からのすべての要求のプロキシミティの計算は同一になります。この方法を使用すると、サイト状況（アベイラビリティ、負荷）およびクライアントとサーバ ゾーン間のネットワーク距離の組み合わせに基づき、最適なサーバが選択されます。

ここでは、次の内容を説明します。

- DNS スティッキ GSLB
- ネットワーク プロキシミティ GSLB

DNS スティッキ GSLB

スティッキ性（別名 ; 固定回答、回答キャッシング）を使用すると、GSS にクライアントの D プロキシから戻った DNS 応答を記憶させ、以降、クライアントの D プロキシから同じ要求がきたときに同一の回答を返すことができます。DNS 規則のスティッキ性を有効にすると、GSS は、要求元のクライアント D プロキシに同一の A レコードの応答を常に提供できるように最善をつくします。こうすることで、元の VIP が常に使用可能であるかのように見せかけます。

GSS の DNS スティッキは、特定のサーバに対する e- コマース クライアントの接続を確実に維持します。クライアントのブラウザが DNS マッピングをリフレッシュした場合であっても処理中であればこの接続は維持されます。ブラウザによっては、ブラウザ インスタンスのライフタイム中（数時間）クライアント接続を維持できますが、それ以外のブラウザは DNS の再解決要求までに 30 分の接続制限が設けられています。この時間は、e- コマース処理を完了しようとしているクライアントにとっては十分ではありません。

ローカル DNS をスティッキにすると、各 GSS デバイスは、同じ GSS デバイスの同じドメイン名に対する以降のクライアント D プロキシの要求を最初の要求と同じロケーションに確実に固定します。DNS スティッキは、GSS を使用して、ユーザ設定のスティッキ非アクティビティ期間中、特定のホステッド ドメインやドメイン リストに対するクライアントの D プロキシのすべての要求が確実に同一の回答を得られるようにして、回答が常に有効であるかのように見せかけます。

グローバル DNS スティッキを有効にすると、ネットワーク内の各 GSS デバイスは、ネットワーク内の他の GSS デバイスの回答を共有し、網目のように完全に接続されたピアツーピアとして動作します。この状態の各 GSS デバイスは、クライアントの D プロキシからの要求と応答を自身のローカル データベースに保存し、ネットワーク内の他の GSS デバイスとその情報を共有します。結果として、ネットワーク内の GSS の同じドメイン名に対する以降のクライアント D プロキシの要求は、クライアントをスティッキの状態にします。

DNS スティッキの選定処理は、DNS 規則の balance 句の一部として開始されます。

ネットワークの GSS デバイスに対するローカルおよびグローバル DNS スティッキの構成方法については、第 8 章「DNS スティッキの設定」を参照してください。

ネットワーク プロキシミティ GSLB

GSS は、要求元の D プロキシに関連したもっとも近接の回答（リソース）で DNS 要求に応答します。ここでは、プロキシミティとは、ネットワーク トポロジ用語で言う、要求元クライアントの D プロキシとその回答間の距離または遅延（地理的な距離ではない）を意味します。

もっとも近接な回答を判断できるように、GSS は各プロキシミティ ゾーンに配置されているプロービング デバイス（Cisco IOS 準拠のルータ）と通信し、要求元クライアントの D プロキシとゾーン間で計測される往復時間（RTT）のメトリック情報を取得します。各 GSS はクライアントの要求を RTT 値が一番低く、かつ使用可能なサーバに誘導します。

プロキシミティの選定処理は、DNS 規則の balance 句の一部として開始されます。要求が有効なプロキシミティを持った DNS 規則と balance 句に一致した場合、GSS はもっとも近い答えで応答します。

ネットワークの GSS デバイスのプロキシミティの設定については、第 9 章「ネットワーク プロキシミティの設定」を参照してください。

DDoS 検出および軽減

Distributed Denial of Service（DDoS; 分散型サービス拒絶）攻撃は、特定のコンピュータやネットワーク リソースへアクセスする正規のユーザを拒絶するように設計されています。これらの攻撃は、数千もの不正な DNS 要求を対象のデバイスに送信する悪意ある攻撃者が原因です。対象のデバイスはこれらの要求を有効なものとして扱うため、DNS は偽の受信者（被害者）に応答します。

対象のデバイスは攻撃者への応答でビジー状態になるため、正規の D プロキシからの有効な DNS 要求が廃棄されます。要求数が数千に及ぶ場合、攻撃者は DNS 応答のマルチギガビット フラッドを生成している可能性が高く、ネットワーク輻輳の原因になります。

ネットワークが輻輳した場合、次の部分でネットワークが影響を受けます。

- 不正な要求の処理でビジー状態になるため、対象のデバイスのパフォーマンスが低下します。
- 応答で生成されたトラフィックがインターネット　バックボーンを横断するため、ISP およびアップストリーム プロバイダーに影響します。
- 不正に使用されたアドレスと類似した IP アドレスを持つホストは、大量のインバウンド DNS トラフィックを受信します。

これらの問題に対処するため、GSS にはライセンスを使用した DDoS 検出モジュールと DDoS 軽減モジュールが用意されています。DDoS ライセンスの取得とインストールについては、『*Global Site Selector Administration Guide*』を参照してください。

一般的に、DDoS モジュールは次の攻撃を防ぎます。

- 攻撃者が被害者（GSS）の IP アドレスを装うリフレクション アタック。詳細については、「軽減規則」を参照してください。
- 不正な形式の DNS パケットが転送される攻撃。
- DNS クエリーが送信される攻撃。
  - 特定の送信元 IP からドメイン（DoS 応答攻撃）に対する攻撃

- GSS で設定されていないドメインへの攻撃
- 全体的な GSS のパケット処理率を上回る、異なる送信元 IP からの攻撃
- 不正な IP アドレスからの攻撃

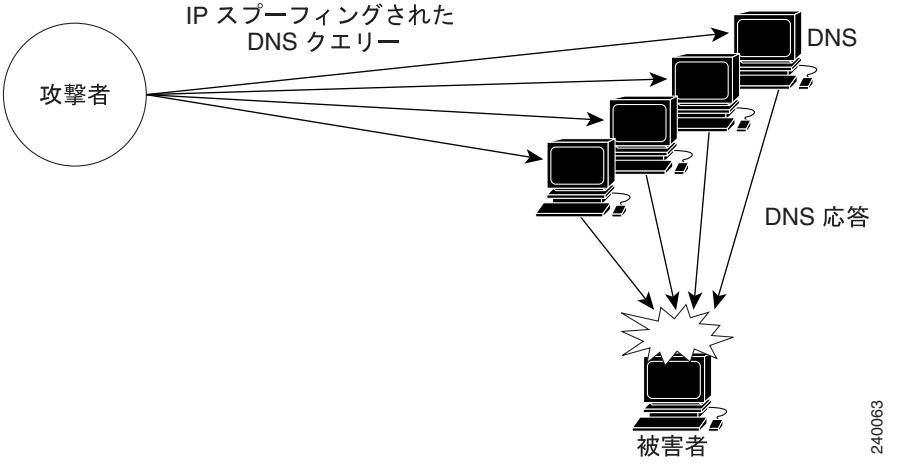
DDoS モジュールは、主に 3 つの機能を使用してこれらの攻撃を防ぎます。各機能については、以降のセクションで説明します。

- 軽減規則
- レート制限
- スプーフィング対策のメカニズム

軽減規則

リフレクション アタックは、攻撃者が被害者（この場合、GSS）の IP アドレスを偽り、複数の DNS 要求を 1 つ以上の DNS サーバに送信することで発生します（図 1-6）。この攻撃は、小さなクエリーは、応答時により大きな UDP パケットを生成するという増幅事実に基づいており、大量の DNS 応答トラフィックで被害者を攻撃します。

図 1-6　　リフレクション アタック図



次の GSS の基本軽減規則を使用すると、この問題の軽減に役立ちます。

- 応答が 53 以外の送信元ポートから着信した場合、送信元ポートが 53 および QR ビットが 1（応答）のパケットを廃棄。
- 応答がポート 53 に着信した場合、宛先ポートが 53 および QR ビットが 1（応答）のパケットを廃棄。
- ペイロード長が 12 バイト未満のクエリーを廃棄。
- 送信元ポートが 53 以上 1024 未満で QR ビットが 0（要求）のパケットを廃棄。

デフォルトでは、軽減規則が有効になっています。

レート制限

GSS は、秒ごとに各 D プロキシの DNS パケット数を制限したり、全体的なレートを制限したりします。他のトラフィックをすべて制限することはありません。はじめは、この制限にデフォルト値が設定されています。ただし、平時であればこの制限を調整したり、D プロキシや D プロキシ グループを設定してこの値を上書きできます。この制限を越えると、DNS パケットは廃棄されます。

（注）　各 D プロキシの最終的なレート制限とグローバルなレート制限は、平時中に学習した（または CLI で設定された）レート制限に許容値をかけることで決定されます。

スプーフィング対策のメカニズム

スプーフィングされたパケットには、送信元デバイスの実 IP アドレスではないヘッダー部に IP アドレスが含まれています。スプーフィングを使用した攻撃の狙いは、目的のサイトのリンクと目的のサイトのサーバ リソースやゾーンを飽和させることです。スプーフィングされたパケットの送信元 IP アドレスは、ランダムに指定されているか、特定の目的を持ったアドレスが指定されています。

スプーフィング攻撃は、Access Control List（ACL; アクセス コントロール リスト）やフィルタを使用して止めることができないため、単一のデバイスからでも簡単に大ボリュームを生成できます。攻撃者は、パケットの送信元 IP アドレスを変更し続ければいいだけです。

GSS は、スプーフィング攻撃に対処できるように、Redirect to TCP と呼ばれるスプーフィング対策メカニズムを使用します。このメカニズムは、DNS クエリーにも使用されており、DNS プロキシと呼ばれています。これは、TCP を使用してクライアントにクエリーを再送信させるメカニズムに基づいています。クエリーが TCP で到着すると、GSS はチャレンジ / レスポンス メカニズムを使用して、送信元を証明します。送信元が証明に成功すれば、GSS は TCP の応答を送信します。D プロキシが UDP で要求を送信した場合、GSS は TC（Truncated）ビット を送信します。D プロキシが TCP で戻せば、GSS は TCP で応答します。

（注）　GSS は、TSIG、DDNS（opcode=5）、DNS 通知要求（opcode=4）を除く、すべての要求パケット（qrbit=0）にスプーフィング対策を提供します。

スプーフィングされたトラフィックとスプーフィングされていないトラフィックを区別することで、チャレンジ / レスポンス アルゴリズムが機能します。GSS はチャレンジ（cookie）を GSS に接続しようとしているクライアントに送信します。パケット ヘッダーの送信元 IP アドレスが、クライアントに割り当てられた IP アドレスの場合、クライアントはチャレンジを受信し、応答を返します。

ただし、パケットの送信元 IP アドレスがスプーフィングされている場合、ゾーンへの元のトラフィックを生成したクライアントは GSS 応答を受信しません。そのため、正しいチャレンジで答えません。GSS は、クライアントが正しいチャレンジを戻したときのみ信頼のおけるクライアントとみなします。DDoS モジュールは、そのようなクライアントからのトラフィックのみ許可し、セレクタまたは CNR に渡します。

DDoS 情報の統計を監視する方法については、第 10 章「GSS GSLB 動作のモニタリング」を参照してください。DDoS 対策を有効にして、フィルタ、レート制限、スプーフィング対策を設定する特定の手順については、『*Cisco Global Site Selector CLI-Based Global Server Load Balancing Configuration Guide*』を参照してください。

GSS のネットワーク配置

一般的な GSS では、企業イントラネットまたはインターネット上に、最大 8 つの GSS デバイスが配置されます。最低 1 つの GSS をプライマリ GSSM として設定する必要があります。また、任意で、2 つめの GSS をスタンバイ GSSM として設定できます。プライマリ GSSM はネットワーク上の他の GSS デバイスを監視し、CLI コマンドまたはセキュア HTTP からアクセスできる GUI を使用して、要求のルーティング サービスの管理と監視を実行する機能を提供します。どの時点においても、アクティブにできるのは 1 つの GSSM のみです。2 番目の GSSM はスタンバイ（バックアップ）デバイスとして機能します。

GSSM 機能は各 GSS に組み込まれています。すべての GSS デバイスは、プライマリ GSSM またはスタンバイ GSSM として機能するように設定できます。

DNS 要求に応答して定期的にキープアライブを送信し、デバイスのリソース ステータス情報を提供する追加の GSS デバイスを GSS ネットワーク上に設定できます。GSS デバイスはプライマリ GSSM ネットワーク管理のタスクを実行しません。

ここでは、GSS の一般的なネットワーク配置と、次の内容について説明します。

- GSS デバイスの特定
- ファイアウォール背後の GSS デバイスの特定
- GSS ノード間の通信
- データセンター内での配置

GSS デバイスの特定

企業がネットワーク内の GSS デバイスの配置を決定することに変わりはありませんが、デバイスの配置時には次の注意事項に従ってください。

GSS は権限ネーム サーバとして 1 つ以上のドメインにサービスするため、各 GSS は企業ネットワーク内でパブリック、またはプライベートに指定できるアドレスを持つ必要があります。こうすることで、コンテンツを要求している D プロキシのクライアントが、DNS 要求を処理するために割り当てられた GSS を検出できます。

ドメインに送受信されるトラフィック パターンに応じて、ドメインの役割を GSS デバイスに委任するオプションを使用できます。たとえば、5 台の GSS デバイスを含むネットワークに対して、ドメインに送信されるすべてのトラフィックが GSS ネットワークに転送されるように、親ドメインの DNS サーバを変更することができます。また、トラフィックのサブセットを 1 つまたは複数の GSS に委任し、その他のトラフィック セグメントを残りのデバイスで処理することもできます。

別の GSS デバイスをネットワークに収容できるようにネットワークの DNS 設定を変更する手順については、第 7 章「DNS 規則の作成および変更」を参照してください。

ファイアウォール背後の GSS デバイスの特定

ファイアウォールを配置すると、GSS ネットワークへの不正アクセスや、GSS デバイスへの一般的な DoS 攻撃を防止できます。GSS は企業のファイアウォールの背後に配置できるだけでなく、パケットフィルタリング機能を備えているため、GSS 管理者はすべての GSS デバイスへのトラフィックを許可したり、禁止することができます。

GSS をファイウォールの背後に配置するか、または GSS 自身のパケット フィルタリングを有効にする場合は、有効なネットワーク トラフィックが GSS デバイスの特定ポートに到達できるように、各デバイス（ファイアウォールおよび GSS）を適切に設定する必要があります。また、プライマリ GSS の GUI にアクセスするためには、HTTPS トラフィックが必要なだけでなく、特定のポートを介して FTP（ファイル転送プロトコル）、Telnet、および SSH アクセスできるように、GSS を設定する必要もあります。さらに、GSS は GSSM に自身のステータスを伝え、そこから設定情報を受信できなければなりません。同様に、プライマリおよびスタンバイ GSSM は相互に通信したり、同期できなければなりません。最後に、グローバル DNS スティッキが GSS ネットワークで有効な場合、網の目のようなスティッキ内のすべての GSS がお互い通信し、スティッキ データベースを共有できる必要があります。

着信トラフィックを制限するアクセス リストについては、『*Cisco Global Site Selector Administration Guide*』を参照してください。GSS を適切に機能させるために、有効にする必要があるポート、および開いたままにしておく必要があるポートについては、「Deploying GSS Devices Behind Firewalls」セクションを参照してください。

GSS ノード間の通信

プライマリ GSSM やスタンバイ GSSM をはじめ、すべての GSS デバイスは DNS クエリーに応答し、GSLB を提供するためにキープアライブを実行します。さらに、プライマリ GSSM は中央集中的な管理デバイスとして機能し、制御する各 GSS の DNS 規則などの共有設定情報を含む、組み込みの GSS データベースをサービスします。GSSM が管理する登録済みの各 GSS デバイスに自動的に通信する設定を変更するには、プライマリ GSSM を使用します。

スタンバイ GSSM は GSS ネットワークの GSLB 機能を実行します。また、スタンバイ GSSM は、指定のプライマリ GSSM が突然オフラインになったり、他の GSS デバイスと通信不能になった場合に、GSS ネットワークで一時的にプライマリ GSSM として機能するように設定されています。プライマリ GSS がオフラインになった場合でも、GSS ネットワークは機能し続けるため、GSLB には影響ありません。

GSS は、プライマリ GSSM で作成された DNS 規則と条件に基づいて DNS クエリーをルーティングします。ネットワ上の各 GSS デバイスは、DNS 要求をサービスする親ドメイン GSS DNS サーバに権限を委任します。

各 GSS はプライマリ GSSM に把握されており、同期をとられます。グローバル DNS スティッキが有効になっていない場合、個々の GSS は互いの存在やステータスを報告しあいません。したがって、GSS が不意にオフラインになっても、同じリソースに処理を行うネットワーク上の他の GSS には影響が及びません。

GSS ネットワークにプライマリとスタンバイの両方の GSSM が配置されている場合、デバイス設定情報および DNS 規則は、プライマリ GSSM とスタンバイ GSSM に保持されているデータ ストア間で自動的に同期されます。

GSS ネットワーク設定が変更されると、2 つのデバイス間で自動的に同期が発生します。更新内容がパッケージ化され、2 つのデバイス間の安全な接続を使用してスタンバイ GSSM に送信されます。

GSS ネットワークの各 GSS デバイスを有効にする手順や、GSS ネットワーク内の GSSM の役割を変更する手順については、『*Cisco Global Site Selector Administration Guide*』を参照してください。

データセンター内での配置

通常、GSS ネットワークは、データセンターやサーバ ファームのような複数のコンテンツ サイトで構成されています。データセンターやサーバ ファームへのアクセスは、Cisco CSS や Cisco CSM のような 1 つ以上の SLB で管理されます。1 つ以上の VIP アドレスは各 SLB を示します。各 VIP は、パブリックにアドレス指定可能なデータセンターのフロントエンドとして機能します。各 SLB の背後にトランザクション サーバ、データベース サーバ、およびミラーリングされた送信元サーバが配置されており、Web サイトからアプリケーションまで、さまざまなコンテンツを提供しています。

GSS は、各 SLB と VIP に関するアベイラビリティと負荷の統計情報を収集し、各データセンターの SLB と直接通信します。GSS はそのデータを使用して、要求をもっとも適切なデータセンターへ誘導し、各データセンター内でもっとも使用できるリソースへ渡します。

一般的なデータセンターには、SLB だけでなく、GSS で管理されない DNS ネーム サーバが配置されている場合もあります。これらの DNS ネーム サーバは、ネーム サーバ転送を使用して、GSS が解決できない要求を解決できます。

GSS ネットワーク管理

GSS ネットワークの管理は、次の 2 つのタイプに分けられます。

- CLI ベースの GSS 管理
- GUI ベースのプライマリ GSSM 管理

特定の GSS ネットワーク管理作業には（初回のデバイス設定、スティッキ グループ設定、近接グループ設定など）、CLI を使用する必要があります。他の作業については、GUI（User Views、Roles など）を使用します。多くの場合、GSLB 設定や監視を実行するために、プライマリ GSSM には GUI または CLI のどちらかを選択できるオプションが用意されています。

CLI の使用と GUI の使用の選択は、個人的または組織的な選択の問題でもあります。また、特定の方法を使用して GSLB 設定を作成し、他の方法を使用して設定を変更できます。

CLI ベースの GSS 管理

CLI を使用すると、GSS で次のインストール、管理、および GSLB タスクを設定できます。

- GSS および GSSM（プライマリ、セカンダリ）デバイスの初回のセットアップおよび設定
- GSS および GSSM 上でのソフトウェアのアップグレードとダウンロード
- データベースのバックアップ、設定のバックアップ、およびデータベースの復旧作業
- プライマリ GSSM での DNS 規則の作成とキープアライブ監視による GSLB 設定および DNS 要求処理

さらに、次のネットワーク設定作業に CLI を使用できます。

- ネットワーク アドレスおよびホスト名の設定
- ネットワーク インターフェイス設定
- IP フィルタリングやトラフィック セグメンテーションなど、GSS デバイスのアクセス制御

また、CLI は各 GSS デバイスに対するステータスの監視およびロギングにも使用できます。

構文やオプション、関連コマンドをはじめ、アルファベット順に記述されているすべての GSS CLI コマンドの一覧は、『*Cisco Global Site Selector Command Reference*』を参照してください。

GUI ベースのプライマリ GSSM 管理

プライマリ GSSM には、GSS ネットワーク全体を監視および管理するための、中央集中型の GUI が 1 つ備わっています。このプライマリ GSSM の GUI を使用して、次のタスクを実行できます。

- DNS　規則を作成し、キープアライブを監視することで、DNS　要求処理と GSLB を設定
- GSS ネットワーク リソースの監視
- 要求ルーティングおよび GSS 統計の監視

GUI の詳細については、「プライマリ GSSM GUI の概要」セクションを参照してください。

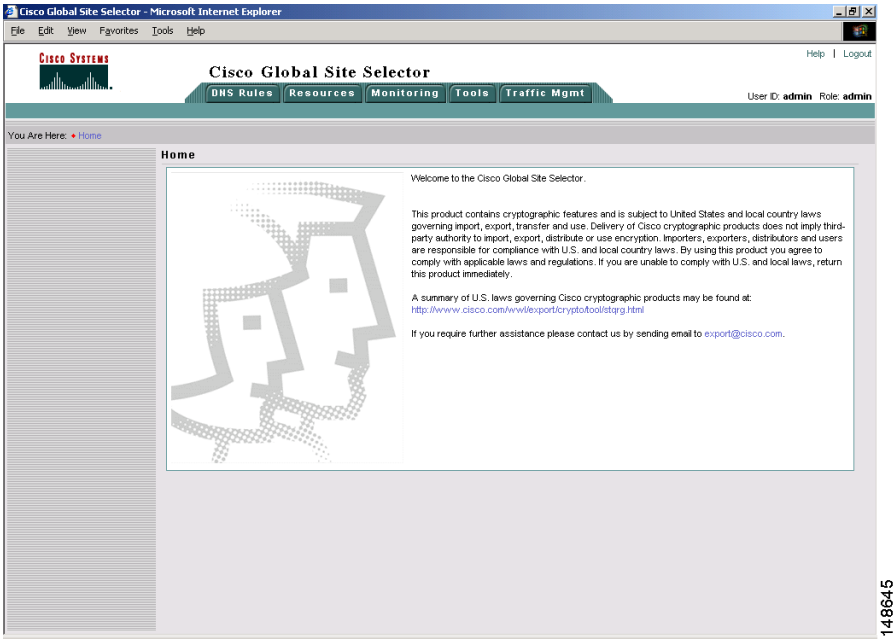
プライマリ GSSM GUI の概要

プライマリ GSSM GUI は、Microsoft Internet Explorer Version 5.0 以降のリリース、Netscape Navigator Version 4.79 以降のリリースなど、任意の標準 Web ブラウザを使用してアクセスする Web ベースのツールです。GUI のアクセス制限には基本認証が使用されています。すべての GUI トラフィックはセキュア HTTP（HTTPS）を使用して暗号化されます。

プライマリ GSSM GUI は、GSS ネットワーク全体の中央管理ポイントとして機能します。プライマリ GSSM GUI を使用すると、使用可能な負荷分散方法の 1 つを使用して、GSS デバイスをネットワークに追加したり、送信元アドレス グループとホステッド ドメインを比較する DNS 規則を作成できます。さらに、GSSM の監視機能を使用すると、GSS ネットワークまたはネットワークの各デバイスのパフォーマンスに関するリアルタイムの統計を取得できます。

プライマリ GSSM GUI へログオン後は、Welcome ウィンドウが表示されます（図 1-7）。現在のログイン アカウント情報が、Welcome ウィンドウの UserID（右上）部分に表示されます。

図 1-7　プライマリ GSSM Welcome ウィンドウ



ここでは、プライマリ GSSM GUI の構成および仕組みについて説明します。

- GUI の構成
- リスト ページ
- 詳細ページ
- ナビゲーション
- プライマリ GSSM GUI アイコンおよび記号
- プライマリ GSSM GUI の Online Help

プライマリ GSSM GUI を使用して GSS ネットワークにグローバル ロードバランシングを定義する前に、この情報に目を通してください。

GUI の構成

プライマリ GSSM GUI は、主に 5 つの部分で構成されています。各部分はタブで分けられており、クリックすることでプライマリ GSSM の特定のセクションへ移動できます。これらの部分を次に示します。

- **DNS Rules タブ** — 送信元アドレス リスト、（ホステッド）ドメイン リスト、回答、回答グループ、共有キープアライブの作成など、DNS 規則の作成および変更を実行するためのページ。
- **Resources タブ** — GSS、ロケーション、リージョン、所有者など、GSS のネットワーク リソースの作成および変更を実行するためのページ。Resources タブからグローバル キープアライブ プロパティを変更することもできます。
- **Monitoring タブ** — 送信元アドレス、ドメイン、回答方法、DNS 規則別のヒット数表示など、GSS ネットワークにおけるコンテンツ ルーティングのパフォーマンスを監視するためのページ。
- **Tools タブ** — ログイン アカウントの作成、アカウント パスワードの管理、システム ログの表示など、GSS ネットワークに関する管理機能を実行するためのページ。
- **Traffic Mgmt タブ** — 高度な GSLB 機能、DNS スティッキ、ネットワーク プロキシミティを設定するページ。

GUI の左上端にある一連のナビゲーション リンクを選択することで、各機能部の特定のページにアクセスできます。ナビゲーション リンクの内容は選択したタブによって異なります。また、ナビゲーション リンクはすべての GUI ページで使用できます。

ページを選択すると、リスト ページと詳細ページで構成された画面が表示されます。リスト ページと詳細ページについては、以降のセクションで説明します。

リスト ページ

リスト ページには機能固有の概要が表示します。たとえば、Answers リスト ページを表示するには、Answers タブ（DNS Rules タブに配置）をクリックします。このリスト ページには、リストされた GSS ネットワークで現在設定されているすべての回答が表示されます。

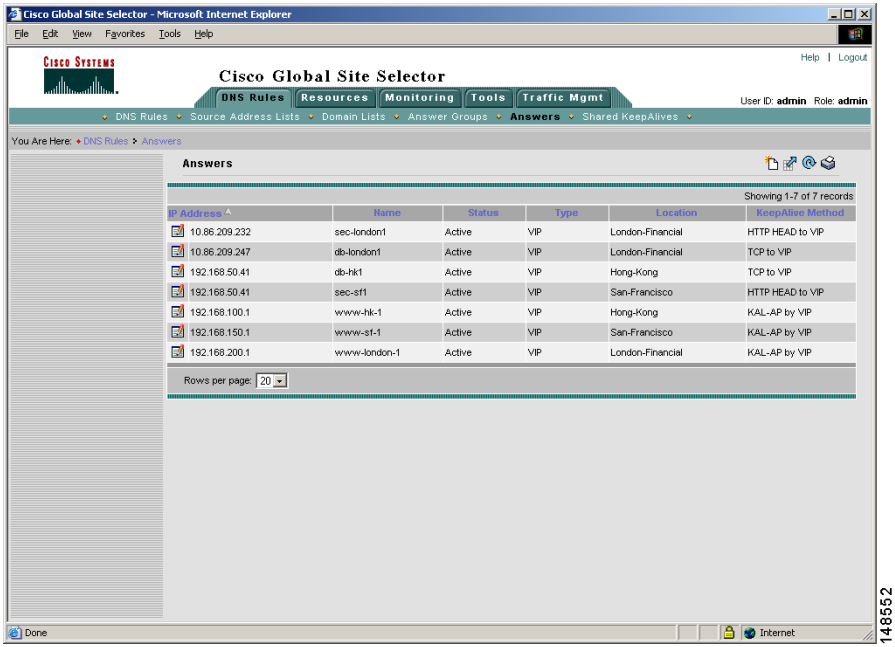
リスト ページはすべてのデータを表形式で表示して、GSS ネットワークで使用できるリソースの詳細表示を提供します。さらに、リスト ページを使用して、新しいリソースを追加したり（DNS 規則、回答グループなど）、既存のリソースを変更したりできます。

リスト ページを使用すると、ページ内にリストされたプロパティ番号の 1 つを使用してリソースをソートできます。名前や所有者、タイプのような識別できる特性を使用すると、特定のリソースをすばやく検出できます。すべてのカラムは昇順または降順で情報をソートできます。リスト ページの情報をソートするには、ソートする情報を含むカラムのカラム ヘッダーをクリックします。

GSS ソフトウェアは、一時的にリスト ページの変更情報を保存するため、リスト ページを維持しながらアクティブなリスト ページに関連した詳細ページに移動できます。アクティブ リスト ページのページごとのソート フィールド、ソート順、および行はメモリ内に一時的に保存されます。他のリスト ページへ移動すると、GSS ソフトウェアは以前のリスト ページの変更内容を破棄します。

図 1-8 に、プライマリ GSSM Answers リスト ページの例を示します。

図 1-8　Answers リスト ページ

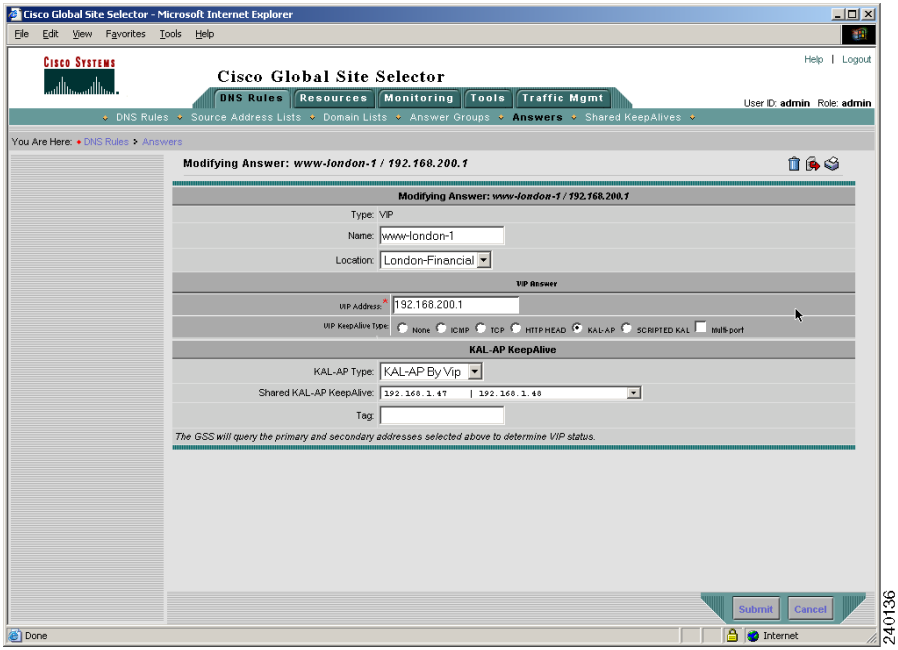


詳細ページ

詳細ページには、特定の GSS 機能の設定情報が表示されます。このページを使用することで、これらのプロパティを定義したり、変更したりできます。詳細ページには、リスト ページからアクセスします。

たとえば、Answers ナビゲーション リンクをクリックし、Answers リスト ページを表示します（図 1-8 を参照）。各回答の横に、メモ帳と鉛筆の形のアイコン（Modify アイコン）があります。Modify アイコンをクリックし、対象の回答の詳細ページを表示します（図 1-9）。Modifying Answer の詳細ページから、回答のプロパティを変更したり、回答を削除したりします。

図 1-9　Modifying Answer の詳細ページ



ナビゲーション

標準ブラウザを使用すると、他と同じような Web ページとしてプライマリ GSSM GUI が表示されます。ただし、プライマリ GSSM GUI ページ間の移動は、異なる Web サイト間の移動や、単一のサイト内での移動とは異なります。他の Web ページとは異なり、主に DNS Rules、Resources、Monitoring、Tools、Traffic Mgmt の各部分のタブを使用して GUI のコンテンツ部分から移動します。Online Help は各ページの上部にナビゲーション リンクとして配置されています。

主要コンテンツ領域内では、ナビゲーション リンクを使用して特定の機能にアクセスしたり、機能間を移動することができます。ナビゲーション リンクで機能を選択すると、即座にその GUI ページに移動します。詳細ページから対応するリスト ページへ戻るには、他のナビゲーション リンクをクリックするか、詳細ページの **Submit** や **Cancel** ボタンをクリックします。

たとえば、GSS デバイスのいずれかの詳細を表示したあとに Global Site Selectors リスト ページに戻るには、異なるナビゲーション リンクをクリックします（または **Cancel** ボタンをクリックします。）。GSS の設定を変更して保存する場合、**Submit** ボタンをクリックします。どちらの操作を行っても、Global Site Selectors リスト ページに戻ります。

（注） Web ブラウザの戻るボタンや進むボタンを使用してプライマリ GSSM GUI のページ間を移動しないでください。**戻る** をクリックすると、プライマリ GSSM に保存されていない変更はすべてキャンセルされます。

プライマリ GSSM GUI アイコンおよび記号

表 1-3 に、プライマリ GSSM GUI で使用される一般的なアイコンと記号、およびその説明を示します。これらのアイコンは、プライマリ GSSM GUI 機能の使用方法を説明するために、このマニュアル全体で使用されます。

表 1-3　GSSM GUI アイコンおよび記号

アイコンおよび記号	目的	場所
	Modify アイコン。関連づけられた項目を編集のために開いて、詳細ページに設定を表示します。	リスト ページ
	Sort アイコン。このカラム内にリストされたプロパティに従って、リスト テーブル内のリスト項目を降順に並べ替えます。	リスト ページ
	Create アイコン /Open DNS Rules Builder アイコン。関連した詳細ページを開き、設定の入力を受け付けます。	リスト ページ

表 1-3　GSSM GUI アイコンおよび記号（続き）

アイコンおよび記号	目的	場所
	Print アイコン。GSS リソースを表示している場合、または GSS ネットワーク アクティビティを監視している場合に、Print アイコンをクリックすると、ローカルまたはネットワーク プリンタを使用して、そのページに表示されているデータを印刷できます。	リスト ページおよび詳細ページ
	Export to CSV アイコン。GSS リソースを表示している場合、または GSS ネットワーク アクティビティを監視している場合に、Export to CVS アイコンをクリックすると、ウィンドウに表示されているデータをカンマ区切りのフラットファイルに保存して、別のアプリケーションで使用することができます。	リスト ページ
	Refresh アイコン。GSS リソースを表示している場合、または GSS ネットワーク アクティビティを監視している場合に、Refresh アイコンをクリックすると、GUI ページのコンテンツが更新されます。	リスト ページ
	Run Wizard アイコン。DNS Rule Wizard を使用して、関連づけられた DNS 規則を編集のために開きます。	DNS Rules リスト ページ
	Filter DNS Rule List アイコン。DNS 規則に適用できるフィルタを提供することで、関心のあるプロパティを持つ規則のみを表示できます。	DNS Rules リスト ページ
	Show All DNS Rules アイコン。すべてのフィルタを削除し、GSS の DNS 規則の完全なリストを表示します。	DNS Rules リスト ページ

表 1-3　GSSM GUI アイコンおよび記号（続き）

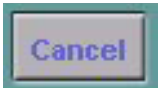
アイコンおよび記号	目的	場所
*	アスタリスク。必須フィールドです。項目を正常に保存するためには、隣接フィールドに値を入力する必要があります。	詳細ページ
	Submit アイコン。設定情報を保存します。特定の GSS システムまたはデバイスの設定情報を編集している際に、Submit アイコンをクリックすると、関連づけられたリスト画面に戻ります。	詳細ページ
	Cancel アイコン。入力された設定変更をキャンセルします。特定の GSS システムまたはデバイスの設定情報を編集している際に、Cancel アイコンをクリックすると、関連づけられたリスト画面に戻ります。	詳細ページ
	Delete アイコン。GSS リソースの設定情報を表示している際に、Delete アイコンをクリックすると、GSS ネットワークからリソースを削除できます。 **（注）** プライマリ GSSM GUI で削除されたものは取り消すことができません。削除したデータを後ほど使用する可能性がある場合、GSSM データベースのバックアップを実行することを推奨します。詳細については、『*Cisco Global Site Selector Administration Guide*』を参照してください。	詳細ページ

表 1-3　GSSM GUI アイコンおよび記号（続き）

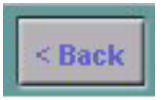
アイコンおよび記号	目的	場所
	Next アイコン。DNS Rules Wizard で、次のページへ進みます。Wizard Contents の目次にあるリンクを使用しても、ウィザードの各ステップに移動できます。	DNS Rules Wizard
	Back アイコン。DNS Rules Wizard で、前のページへ戻ります。Wizard Contents の目次にあるリンクを使用しても、ウィザードの各ステップに移動できます。	DNS Rules Wizard
	Finish アイコン。変更内容を DNS 規則に保存します。DNS Rules リスト ページに戻ります。	DNS Rules Wizard
	Click to Add KAL アイコン。単一の VIP タイプの回答に複数のキープアライブおよび（または）宛先ポートを追加します。	Creating Answer および Modifying Answer の詳細ページ
	Activate Answer アイコン。1 つの中断中の回答、回答グループ内のすべての中断中の回答、所有者に関連付けられたすべての中断中の回答、ロケーションに関連付けられたすべての中断中の回答を再アクティブ化します。	Modifying Answer、Modifying Answer Group、Modifying Owner、Modifying Location の詳細ページ

表 1-3　GSSM GUI アイコンおよび記号（続き）

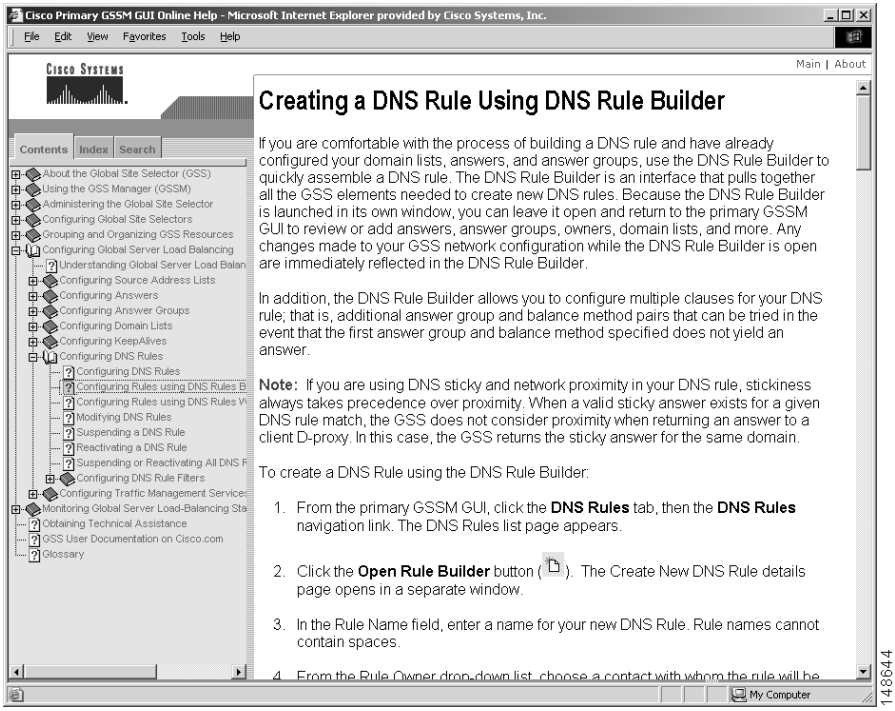
アイコンおよび記号	目的	場所
	Suspend Answer アイコン。GSS の 1 つの回答、回答グループ内のすべての回答、所有者のすべてのグループのすべての回答、ロケーション内のすべての回答を一時的に中断します。	Modifying Answer、Modifying Answer Group、Modifying Owner、Modifying Location の詳細ページ
	Activate DNS Rule アイコン。1 つの中断中の DNS 規則、所有者に関連付けられたすべての中断中の DNS 規則を再アクティブ化します。	Modify DNS Rules および Modifying Owner の詳細ページ
	Suspend DNS Rules アイコン。単一の DNS 規則、または GSS の所有者に関連付けられたすべての中断中の DNS 規則で処理中の要求を一時的に停止します。	Modify DNS Rules および Modifying Owner の詳細ページ
	Set Answers KAL ICMP アイコン。選択された共有のキープアライブからすべての回答の関連を解除し、回答に関連した VIP を使用して各回答のキープアライブ タイプを ICMP に設定します。	Modifying Shared Keepalive の詳細ページ
	Set Answers KAL None アイコン。選択された共有のキープアライブからすべての回答の関連を解除し、各回答のキープアライブ タイプを None に設定します。GSS は 回答が常に有効であると想定します。	Modifying Shared Keepalive の詳細ページ

プライマリ GSSM GUI の Online Help

各プライマリ GSSM GUI ページの右上端にある Help ナビゲーション リンクをクリックすると、Online Help システムが起動します（図 1-10）。この Online Help には、プライマリ GSSM GUI の機能だけでなく、ページの使用方法に関する情報も含まれています。フォームに関連付けられた Online Help トピックが、別途子のブラウザ ウィンドウに表示されます。

プライマリ GSSM GUI の各ページには、そのページに関連したコンテキスト オンライン ヘルプ ファイルが用意されています。これらの Help ファイル（HTML 形式）には、使用しているフォームに関連した詳細情報が記述されています。Online Help には、一連のクイック スタート手順も含まれています。クイック スタートを使用すると、ユーザ インターフェイスの特定のフォームを使用しての移動や、特定の設定手順（DNS Rules Wizard を使用した DNS 規則の作成など）の実行を簡単に行えます。

図 1-10　プライマリ GSSM GUI の Online Help



GSS Online Help システムには、複数のナビゲーション エイドが用意されており、必要な情報の検出をすばやく簡単に行えます。ナビゲーション フレームは、各 Help トピックの左フレームに配置されています。ナビゲーション フレームには、次の 3 つのタブがあります。

- **Contents** — GSSM Online Help システムのすべてのトピックを段状に表示します。Help トピックは機能ごとにグループ化された論理ブックです。Help トピックのブックには、追加トピックとしてサブブックが含まれることがあります。コンテンツは必要に応じて展開したり閉じたりできます。また、コンテンツは現在表示している Help トピックと自動的に同期をとることにも注意してください。

- **Index** — 用語の一覧を表示します。本の背面の索引と類似しており、キーワードに基づいたトピックを探すことができます。索引エントリに関連したトピックが 1 つだけの場合、そのエントリをダブルクリックすると、そのトピックが即座に表示されます。1 つ以上のトピックが索引エントリに関連付けられている場合、Help システムに Topics Found ダイアログ ボックスが表示されます。このダイアログ ボックスを使用することで、トピック リストから表示させるトピックを選択できます。
- **Search** — テキストを使用した検索ツールです。テキスト ボックスに入力した用語に関連する Help トピックのリストが表示されます。トピックを選択したら **Display** をクリックして、そのトピックを表示させます。

GSLB の概要

GSSM（プライマリ、セカンダリ）および GSS デバイスを作成し、ネットワークに接続するように設定したら、GSS ネットワークに要求ルーティングおよび GSLB を設定する準備は完了です。GSS（プライマリ、セカンダリ）および GSS デバイスのセットアップ手順、設定手順、GSLB の準備については、『*Cisco Global Site Selector Getting Started Guide*』を参照してください。

GSS ネットワークに GSLB を設定するには、プライマリ GSSM の中央集中型の GUI を使用します。また、このインターフェイスを使用し、ネットワーク上の SLB とサーバの状態を監視するためにキープアライブを設定します。

アベイラビリティが最も高いデータセンターおよびネットワーク上のリソースに着信 DNS 要求をルーティングする DNS 規則を作成します。したがって、DNS 規則の構成要素を設定してから、規則自体を作成する必要があります。

プライマリ GSSM から GSLB の GSS デバイスとリソースを設定する場合、次の手順を使用してください。

1. リージョン、ロケーション、所有者を作成します（オプション）。これらのグループを使用して、GSS ネットワーク リソースをカスタマー アカウント、物理的な位置、所有者、またはその他の編成方法別に編成します。詳細については、第 2 章「リソースの設定」を参照してください。
2. 送信元アドレス リストを 1 つまたは複数作成します（オプション）。これらの IP アドレスのリストを使用して、指定のドメインの要求を転送するネーム サーバ（D プロキシ）を特定します。デフォルトの送信元アドレス リストは Anywhere で、ドメインに着信するすべての DNS 要求を照会します。詳細については、第 3 章「送信元アドレス リストの作成」を参照してください。
3. ドメイン リストを 1 つまたは複数作成します。GSS による管理およびユーザからの問い合わせを受けるインターネット ドメインのリストを、通常は、ワイルドカードを使用して作成します。詳細については、第 4 章「ドメイン リストの設定」を参照してください。
4. デフォルトのグローバル　キープアライブ設定を変更したり、共有キープアライブを作成したりします（オプション）。GSS ネットワーク リソースは、キープアライブにリンクされた 1 つまたは複数の GSS リソースのオンライン ステータスを監視するために、定期的にポーリングされます。共有キープアライブは、KAL-AP キープアライブ タイプを使用するすべての回答で必要になります。詳細については、第 5 章「キープアライブの設定」を参照してください。

5. 1 つまたは複数の回答と回答グループを作成します。回答は、ドメインへの要求を照会するリソースです。回答グループはコンテンツの要求をそれぞれに分けたリソースの集まりです。詳細については、第 6 章「回答および回答グループの設定」を参照してください。
6. GSS ネットワークで GSLB を管理する DNS 規則を構築します。詳細については、第 7 章「DNS 規則の作成および変更」を参照してください。
7. GSLB に DNS スティッキを使用する場合、ネットワーク内の GSS デバイスにローカルまたはグローバルな DNS スティッキを設定します。スティッキ性を使用すると、GSS にクライアントの D プロキシから戻った DNS 応答を記憶させ、以降、クライアントから同じ要求がきたときに同一の回答を返すことができます詳細については、第 8 章「DNS スティッキの設定」を参照してください。
8. GSLB にネットワーク プロキシミティを使用する場合、ネットワークの GSS デバイスのプロキシミティを設定します。プロキシミティを設定すると、グローバル ロードバランシング要求を処理する際に、最善の（最適な）リソースを特定できます。詳細については、第 9 章「ネットワーク プロキシミティの設定」を参照してください。

次の作業

第 2 章「リソースの設定」では、ロケーション、リージョン、所有者で GSS のネットワーク リソースを編成する方法を説明します。

次の作業