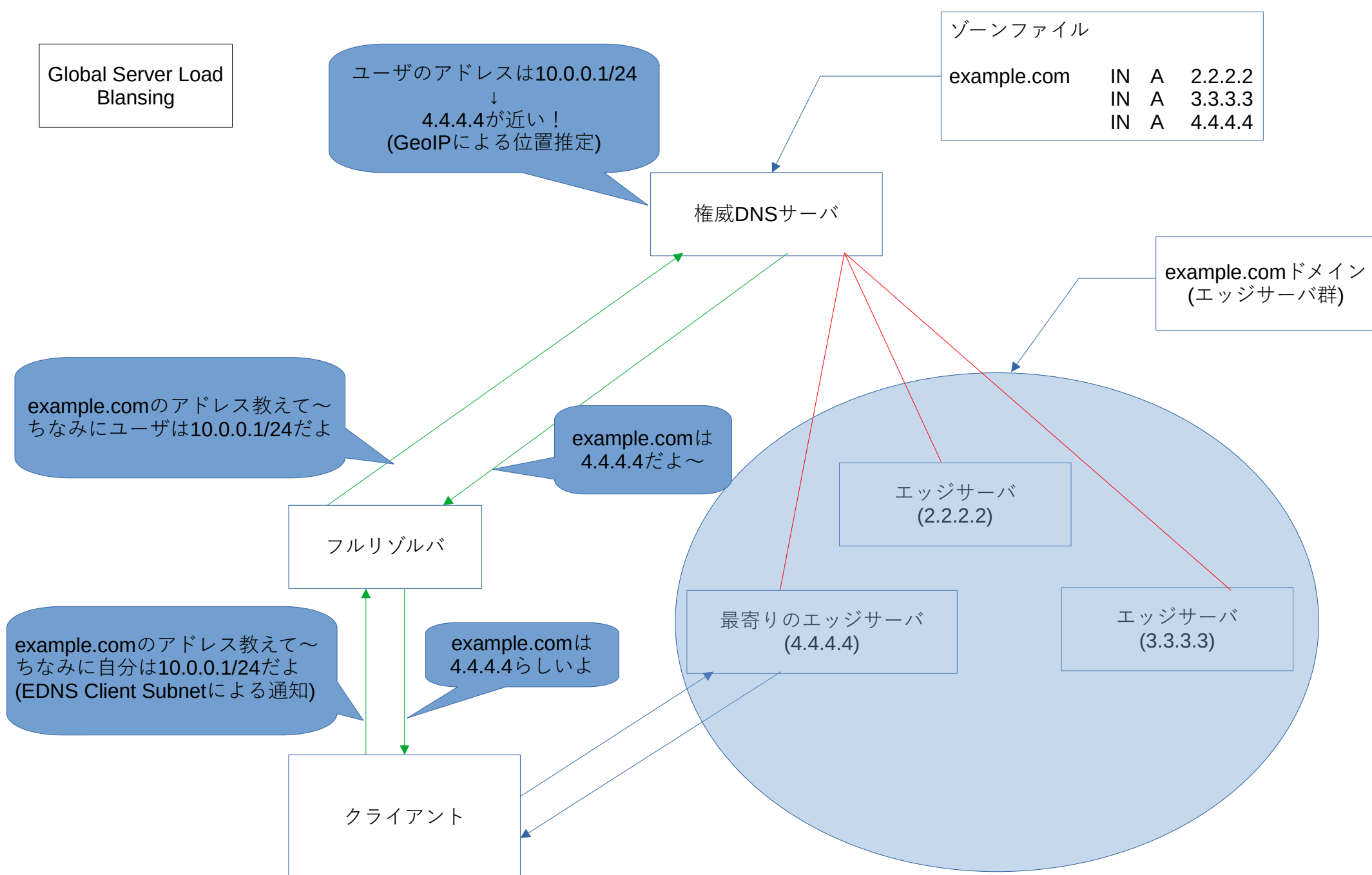


GSLBに特化した権威DNSサーバ用ソフトウェア

fubuki

開発駆動コース仲山ゼミ
川杉倫太郎



GSLB(Global Server Load Balancing)とは分散配置されたエッジサーバ群からなるシステムに対して、権威DNSサーバを制御点としてヘルスチェック、負荷状況、レイテンシや地理的的近接性に基づきDNSのレスポンスを制御することでトラフィックを動的に振り分ける負荷分散システムです。

GSLBをオンプレミスで構築する手段は

- ・専用機器を使う
- ・GSLBに特化した権威DNSサーバを使う

の2通りあり、前者は現状開発されているOSSが一つしかなく後者はコストが高いということもあり現状は難易度が高く折角の素晴らしい負荷分散システムがとても勿体ない状況に置かれていると考え「GSLBをより自由に味わえるソフトウェア」を目指して「fubuki」を開発しました。

GSLBは

- ・負荷分散制御
- ・ヘルスチェック
- ・DNS

の三点からなり、fubukiではこれらの要素を主眼に置いて開発しました。

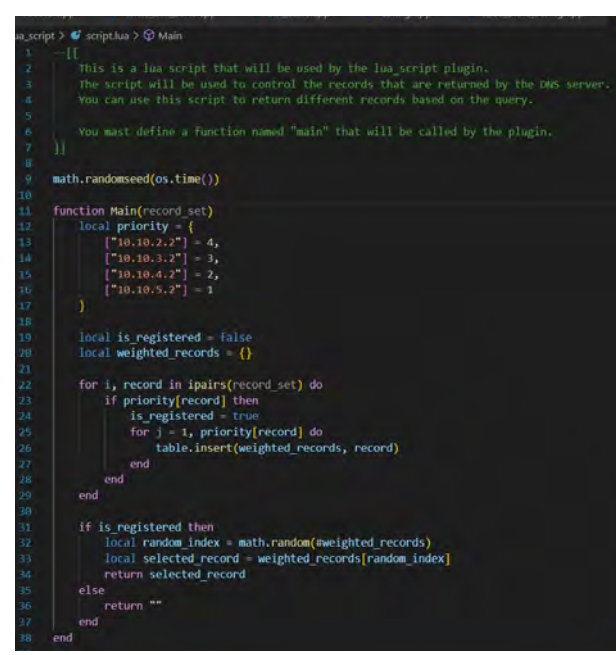
Luaでの負荷分散制御

GSLBの根幹は負荷分散制御です。

fubukiでは従来の負荷分散制御を超えた、圧倒的に柔軟で自由度の高い負荷分散制御をLuaによって可能にしています。これによりLuaからアクセスできるあらゆる要素での制御が可能になり、以下の表のように、例えばヘルスチェックで取得した各サーバのヘルスデータを元にリアルタイムでの負荷分散を行ったり、IPアドレスのブラックリストなどを用いたDNSレベルでのWAFとして動作させることも可能です。

ドメインというシステムにおいてDNSは誰しもが利用する、サーバとクライアントを繋ぐ接続点であり、それはすなわちクライアントとサーバの両方にアプローチした制御点となりうるという事です。fubukiはその性質を最大限活用し、これまでにない負荷分散を可能にします

制御方法	負荷分散の目的	シチュエーション	制御要素
重み付け	サーバ能力に応じた分散	サーバ間の能力差を持つ環境での効率的なリソース活用	サーバIP + トラフィック比率(weight)
ヘルスチェック	障害回避・信頼性向上	サーバ障害時のリカバリー・ユーザ体験の向上	サーバIP + 稼働状況 + 応答速度(RTT, latency)
地理的制御	レイテンシ削減・地域別最適化	グローバル展開されたシステムでの最適化	クライアントIP + GeolP + 地域別優先サーバ
リソース負荷	パフォーマンス最適化・ボトルネック回避	高トラフィック時の全体的な負荷の分散	CPU使用率 + アクティブ接続数 + サーバIP
時間制御	コスト最適化・ピーク時間対応	特定時間帯のトラフィックを重点的に分散	現在時刻 + 時間帯別優先サーバ
フェイルオーバー	高可用性の確保	サーバ障害時の迅速な切り替えでシステム停止を回避	稼働状況 + 代替サーバIP



IPアドレスのリストの重み付けによる負荷分散制御の例
Luaにより30行ほどで記述可能

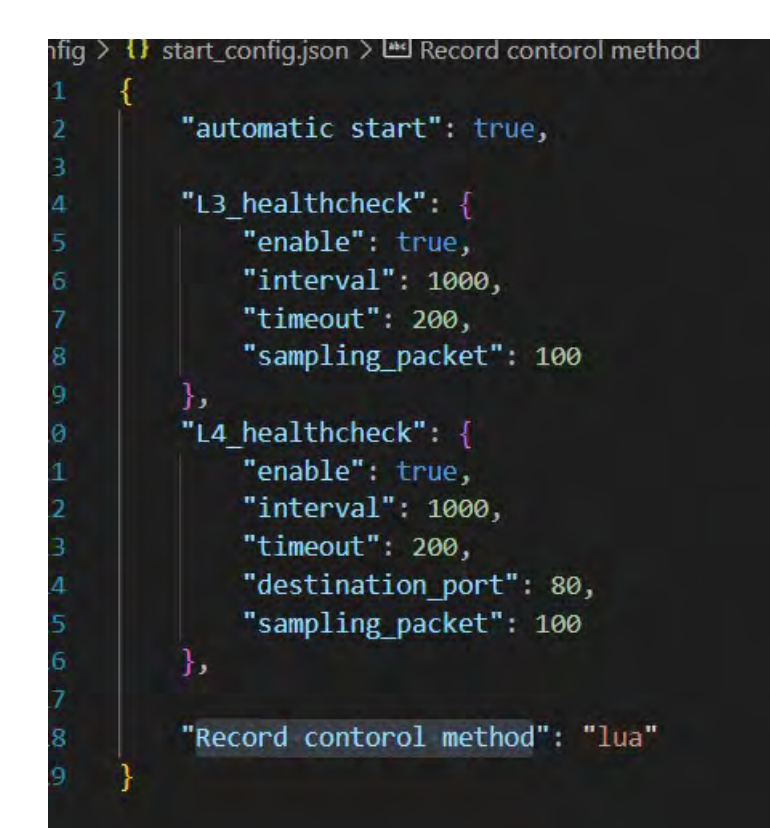
ヘルスチェック

GSLBの根幹を支え、ドメイン全体を監視運用するための要がヘルスチェックです。

fubukiではL3(ICMP)とL4(TCP,任意ポート)でのヘルスチェックに対応しており、それぞれを並列で行える他に全てのヘルスチェックにおいて送信間隔とタイムアウトをそれぞれミリ秒単位で、またサンプリングパケット数をそれぞれ設定することが可能です。これによりヘルスチェック自体を柔軟に運用する事が可能になります。

fubukiではさらにL3,L4の両方においてRTTの平均値と中央値、パケットロス数と割合をリアルタイムで取得する事が可能です。これらのヘルスデータを組み合わせる事で約230通りもの高度なサーバ稼働状況のデータを構築することができ、それらを用いることでfubukiの高度な負荷分散制御の要素として重要な役割を果たしています。

また簡易的な負荷分散制御のコンフィグとして取得したヘルスデータを用いることができます。これにより取り敢えずGSLBを動かしてみたいという状況でもすぐに使用することが可能です。



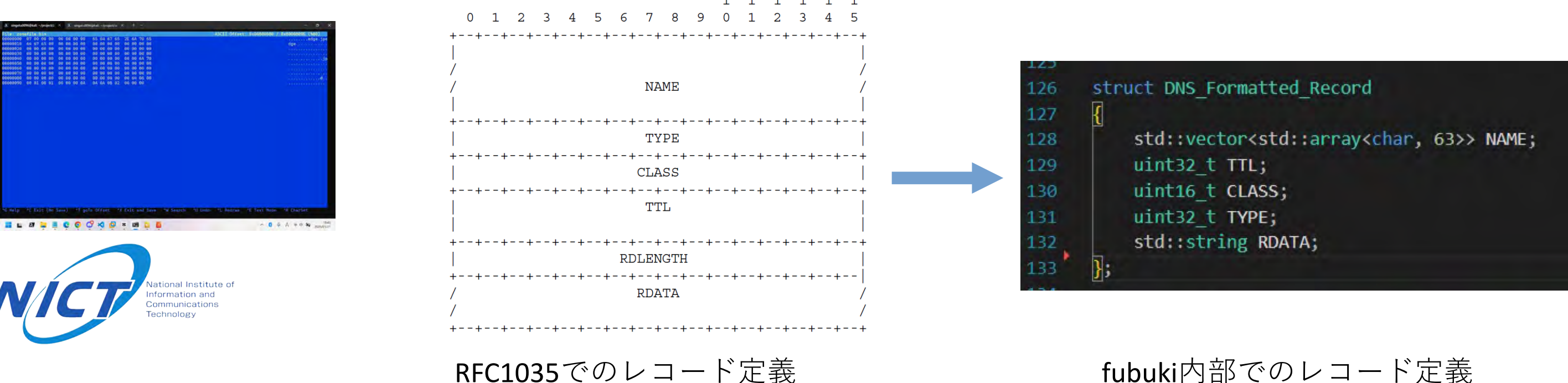
ヘルスチェックコンフィグ



簡易コンフィグ

レコードの管理、操作

GSLBは通常権威DNSサーバを用いた負荷分散システムでありDNSを構築することは不可欠でありDNSはGSLBの基礎となります。fubukiは権威DNSサーバ機能をフルスクラッチで実装することでよりGSLBに特化した権威DNSサーバを基盤としています。GSLBは巨大なシステムに対して用いられることが多く、膨大なレコードが常に書き変わりがながら運用されることが考えられます。この事を考慮し、fubuki内部ではドメイン構造を再現したインメモリデータベースを構築することでより高速かつ直感的な操作を可能にしています。またこれらを使用することで稼働中にリアルタイムでレコードの追加、変更の反映を可能にしています。ゾーンファイルは従来のbindなどで用いられるテキスト形式ではなくバイナリ形式とすることで構文解析が不要になり、文法ミスなども防がれます。



RFC1035でのレコード定義

fubuki内部でのレコード定義

まとめ

fubukiは「GSLBをより自由に味わえるソフトウェア」を目指して開発されました。現状ではGSLBを自由に味わうのに十分な柔軟性や可用性を持ち合わせていると考えています。またfubukiはシステム全体の制御点となることからDNSレイヤでのWAFのように使用することも可能であり、セキュリティの向上へも寄与します。このようにfubukiは語源となった白上フブキさんのように様々な可能性を秘めています。この先も、その可能性をより広げていければと思います。

今後の展望

現状fubukiはまだ知名度が低く、一般の人が用いるのにはハードルが高いためドキュメントの整備などを進めより多くの人にGSLBを使ってもらい、その魅力をより感じ取って貰いたいと思います。

この場をお借りして一年間を通してサポートしてくださったSecHack365のトレーナー、事務局の方々と、共に走り抜いたトレーニーの方々へ深い感謝を述べさせていただきます。一年間大変お世話になりました。