【DNS】少人数での自前運用からDistributed Cloud DNSに切り替えることにした話

田中 温子
技術部
株式会社ミライコミュニケーションネットワーク

少人数での自前運用から Distributed Cloud DNSに 切り替えることにした話

App World 2024

株式会社ミライコミュニケーションネットワーク
田中温子

今日のお話

- 権威DNSサーバの自前運用に限界を感じる日々・・・
- 外部の権威DNSサービスへ移行したいけど、自社システムとのしがらみがあり、コストも限られている
- なぜDistributed Cloud DNSを選んだのか
- 実際に使ってみてどうか

自己紹介

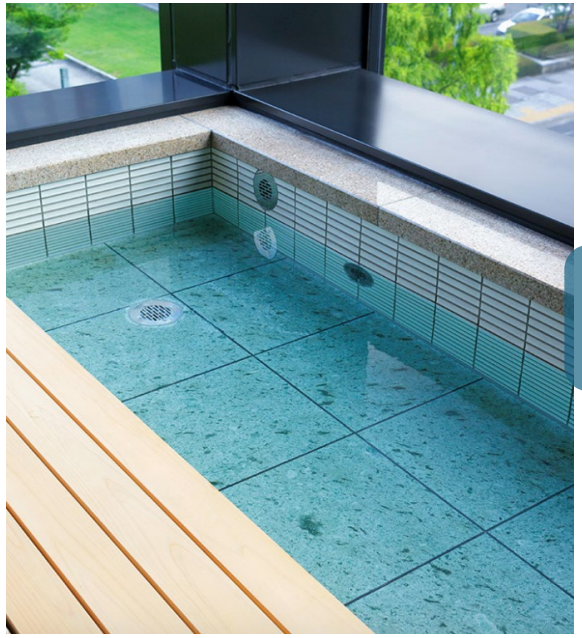
名前：　田中温子
所属：　ミライコミュニケーションネットワーク
　　技術部運用チーム
仕事：　サーバーエンジニア

- ホスティングサーバの設計構築、障害対応
- メールサーバのリプレースをよくやっている

活動：　ChuNOGコアメンバー、DNSOPS.jp
趣味：　ハリネズミの観察

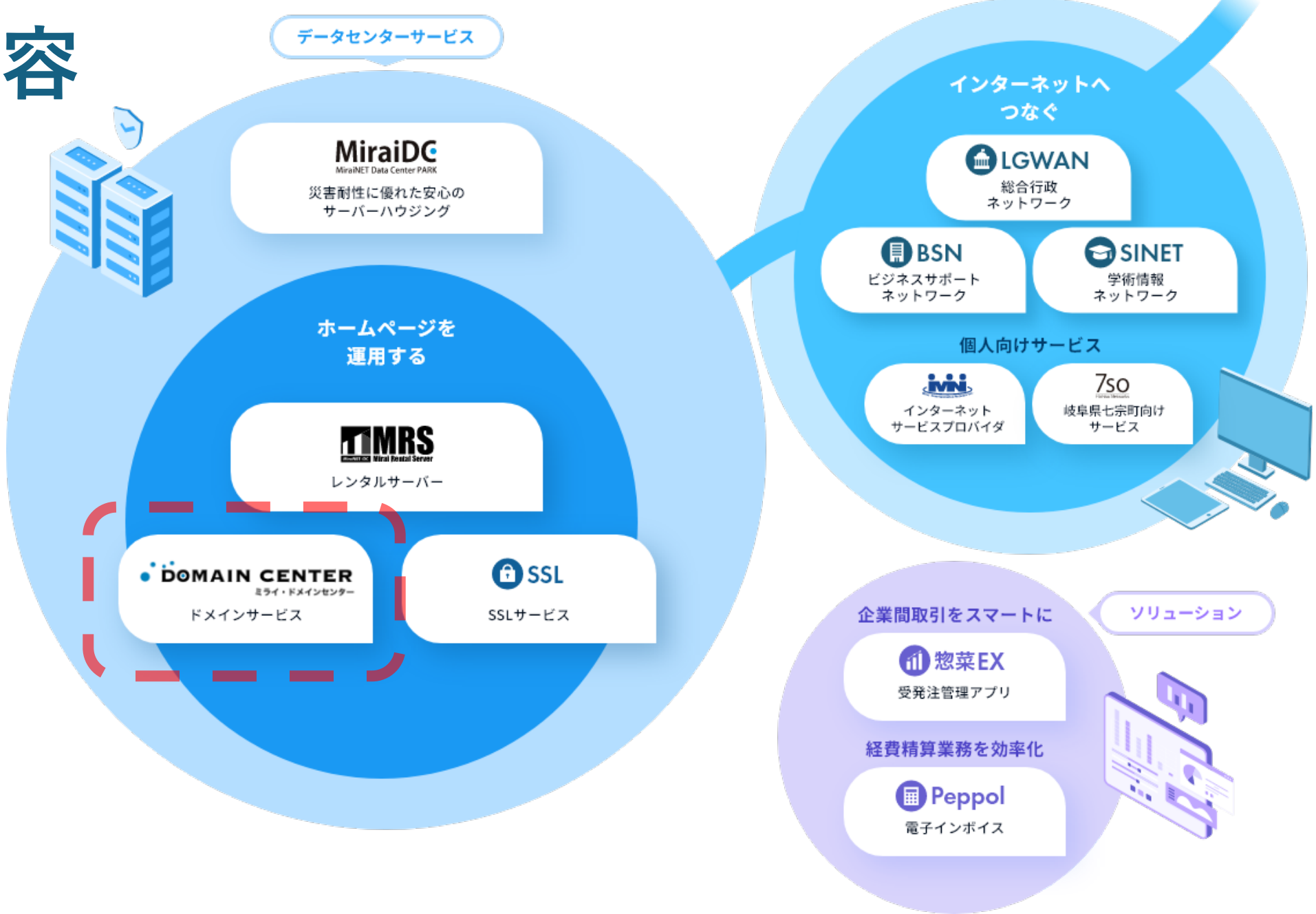
会社紹介

社名　：　株式会社ミライコミュニケーションネットワーク
所在地：　岐阜県大垣市
設立　：　2001年
社員数：　33名



岐阜県にある足湯のあるデータセンター

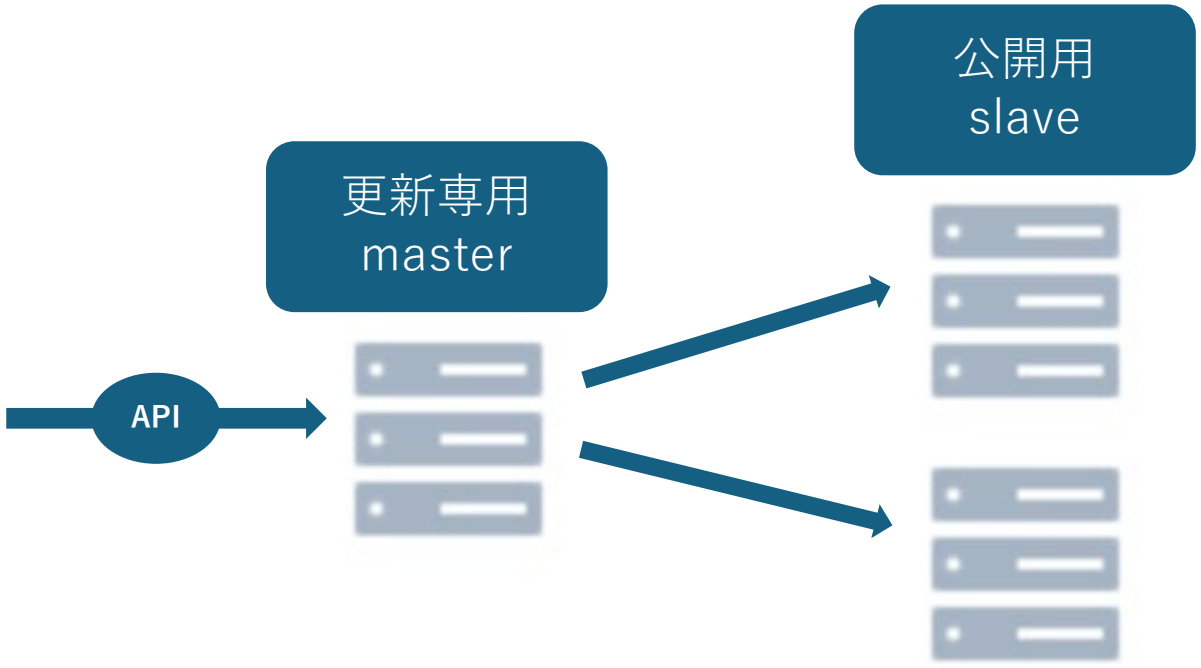
事業内容


データセンターサービス
MiraiDC
MiraiNET Data Center PARK
災害耐性に優れた安心の
サーバーハウジング
ホームページを
運用する
MRS
Mirai Rental Server
レンタルサーバー
DOMAIN CENTER
ミライ・ドメインセンター
ドメインサービス
SSL
SSLサービス
ネットワークサービス
インターネットへ
つなぐ
LGWAN
総合行政
ネットワーク
BSN
ビジネスサポート
ネットワーク
SINET
学術情報
ネットワーク
個人向けサービス
IVNI
インターネット
サービスプロバイダ
7so
岐阜県七宗町向け
サービス
ソリューション
企業間取引をスマートに
惣菜EX
受発注管理アプリ
経費精算業務を効率化
Peppol
電子インボイス

既存システムの課題

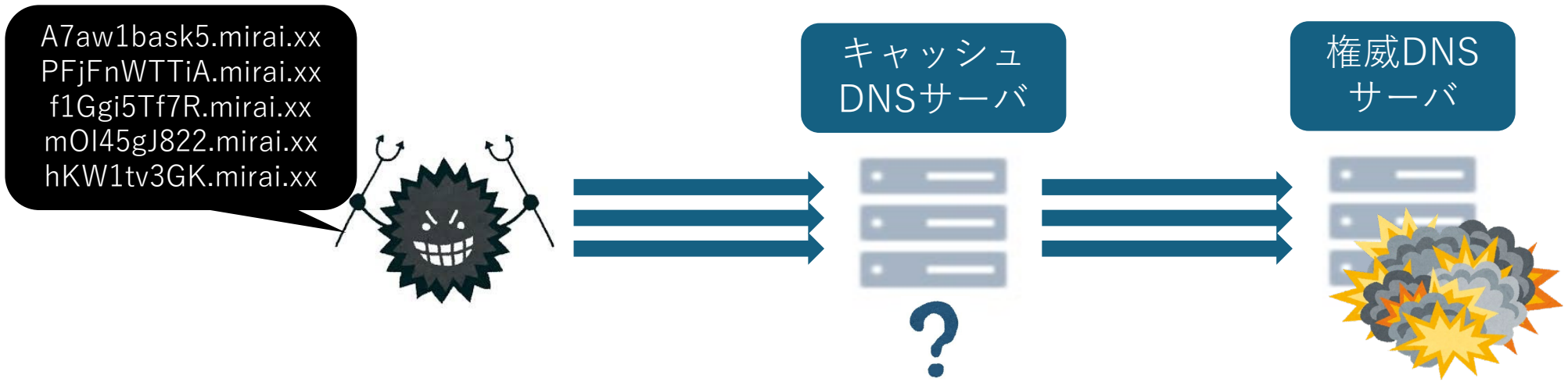
既存の権威DNSサーバの構成

- OSSで構築した権威DNSサーバが複数セット存在
- レコード編集ができるドメイン管理画面を顧客へ提供
- ドメイン数は約2500



権威DNSサーバへの攻撃

- 2023年頃から、権威DNSサーバに対してランダムサブドメイン攻撃を受けるようになる
- 2023年12月には、攻撃による名前解決不能が原因で、Webやメールサービスに障害が発生した



ランダムなサブドメインの名前解決を大量に送りつけてサービスダウンに追い込む

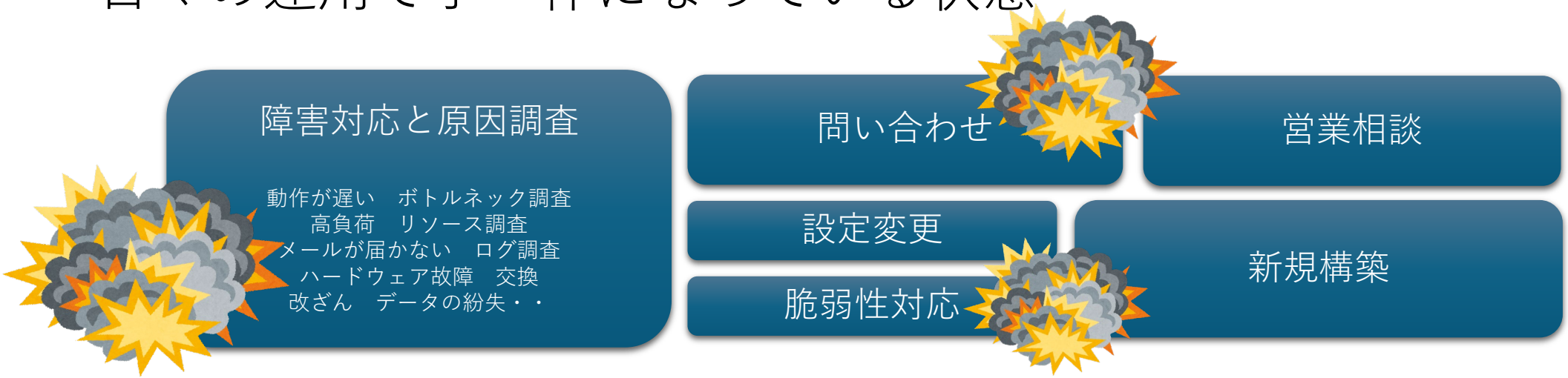
攻撃への対処

- ランダムサブドメイン攻撃に対して、以下のような抜本的な対処は行えずにいた
  - 多数のクエリを捌けるよう権威DNSサーバのパフォーマンスの強化
  - レートリミットをかけて過剰な名前解決を防ぐ
  - DNSに対応したDDoS Mitigation製品の導入

- 実際は場当たり的な対処しかできていなかった
  - 多数クエリを送ってくるIPアドレスをブロック
  - TTLを適切な値に設定

運用の課題

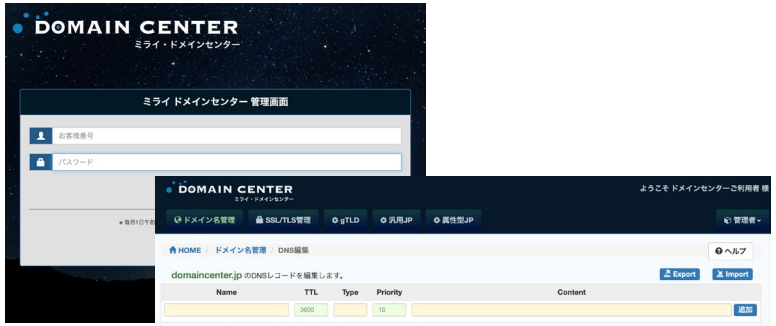
- ホスティングサーバの構築・運用を行うメンバーは9名
  DNSの専門チームはなし
- 日々の運用で手一杯になっている状態・・・

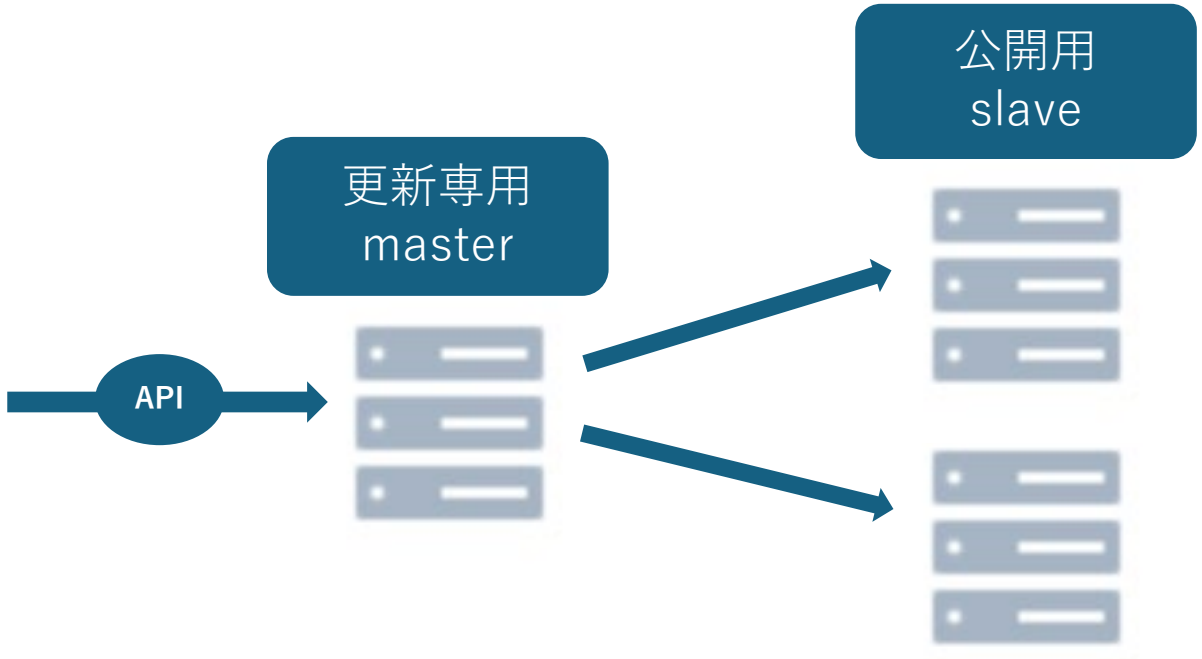


自分たちで調査・検証して対処をすることに限界を感じ、
外部の権威DNSサービスの検討を始める

自社開発システムとのしがらみ

- 自社開発のドメイン管理画面が複数あり、顧客に提供している
- 自社開発のAPIが、権威DNSサーバのレコード情報を書き換える





顧客向けのインタフェースは変更できないため、外部の権威DNSサービスを使うにはAPIの改修が必要

Distributed Cloud DNSに決めるまで

まず検討したDNSファイアウォール

- 以下の理由から、最初はDNSファイアウォールを検討した
  - なるべく早く導入したい
  - 自社開発システムのAPIの改修はすぐにできない

- 見積もりをもらうための情報を準備
  - ドメイン数
  - 1ヶ月あたりのクエリ数
- 3社から見積もりをもらう
- この中のA社に発注することを決め、社内稟議も通した
- A社への発注直前に、F5 Distributed Cloud DNSの存在を知る

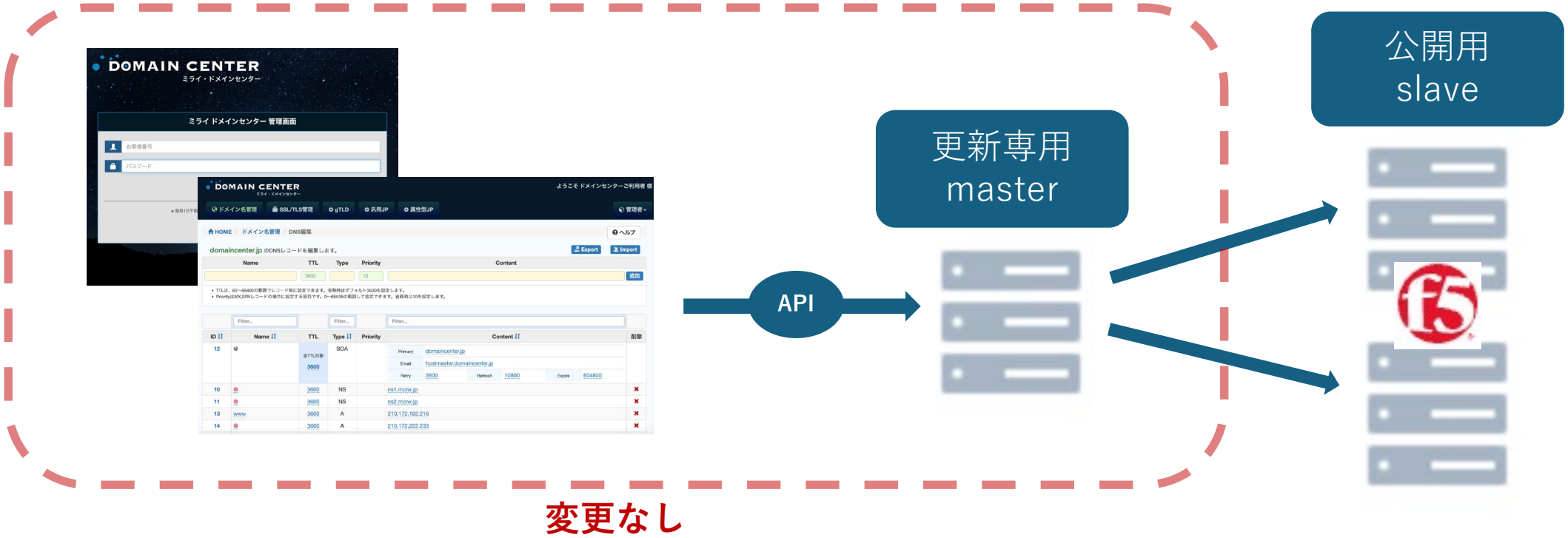
Distributed Cloud DNSを選んだ理由

セカンダリを受けて
hidden master構成が取れる

クエリ数での課金がなく
ドメイン数での課金体系

セカンダリを受けてhidden master構成

- 既存の権威DNSサーバからゾーン転送、セカンダリのみを公開し、外部からの問い合わせを受け付ける構成
- 顧客向けのインタフェース、APIの改修なしで導入が可能

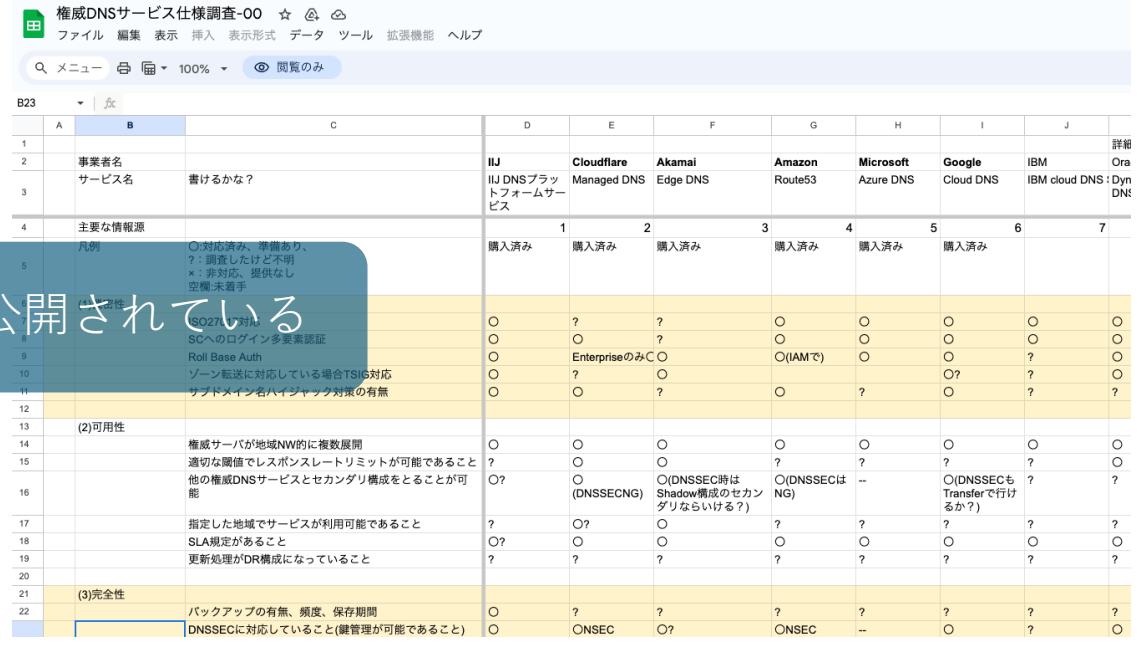


クエリ数ではなくドメイン数での課金

- DNSファイアウォールや、権威DNSサービスは、クエリ数で課金するものが多い
- 地方自治体など官公庁の場合、年度ごとに予算が決まっており、年度ごとの発注になる
- クエリ量によって変動したコストを追加請求できない
- ドメイン数での課金であり、契約期間中の追加課金がないのは大きなポイントになった

他社の権威DNSサービスとの比較

- 外部の権威DNSサービスを選ぶ時に、何が違うのか？コスト以外にどういう観点で比較すればいいのか？は悩むもの
- DNSOPS.jp（日本DNSオペレーターズグループ）で行った権威DNSサービス調査を参考にした

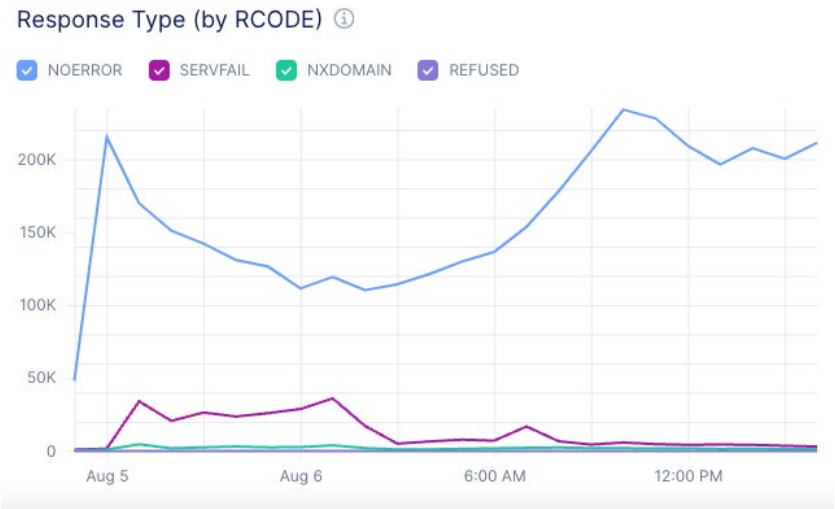


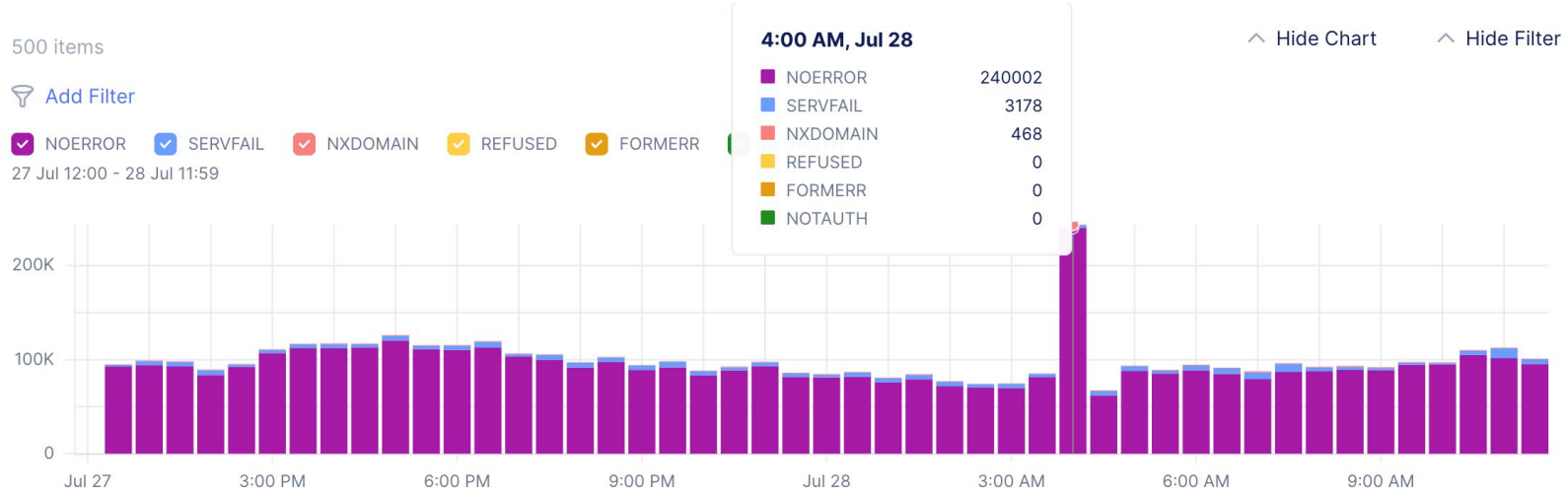
調査報告書は公開されている

Distributed Cloud DNSを実際に使ってみて

ここがいい

- セカンダリ構成での導入は3ステップで完了
- Performance表示がわかりやすい
- 一時的ではない検証環境の提供
- F5のエンジニアの親しみやすく、柔軟なサポート





ここはもっと良くなることを期待

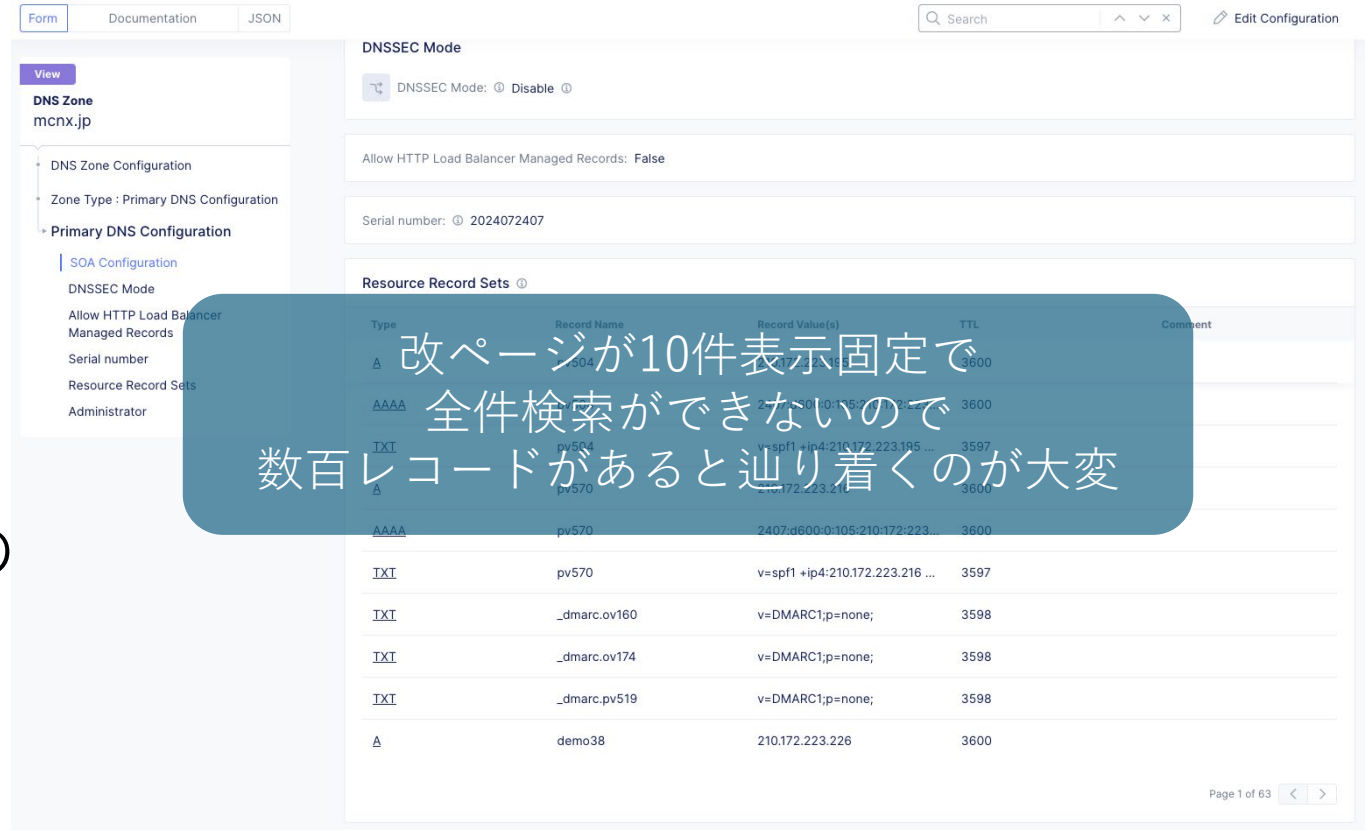
- リソースレコードの
  表示が10件ずつで固定

→リクエスト

→改善していただいた！

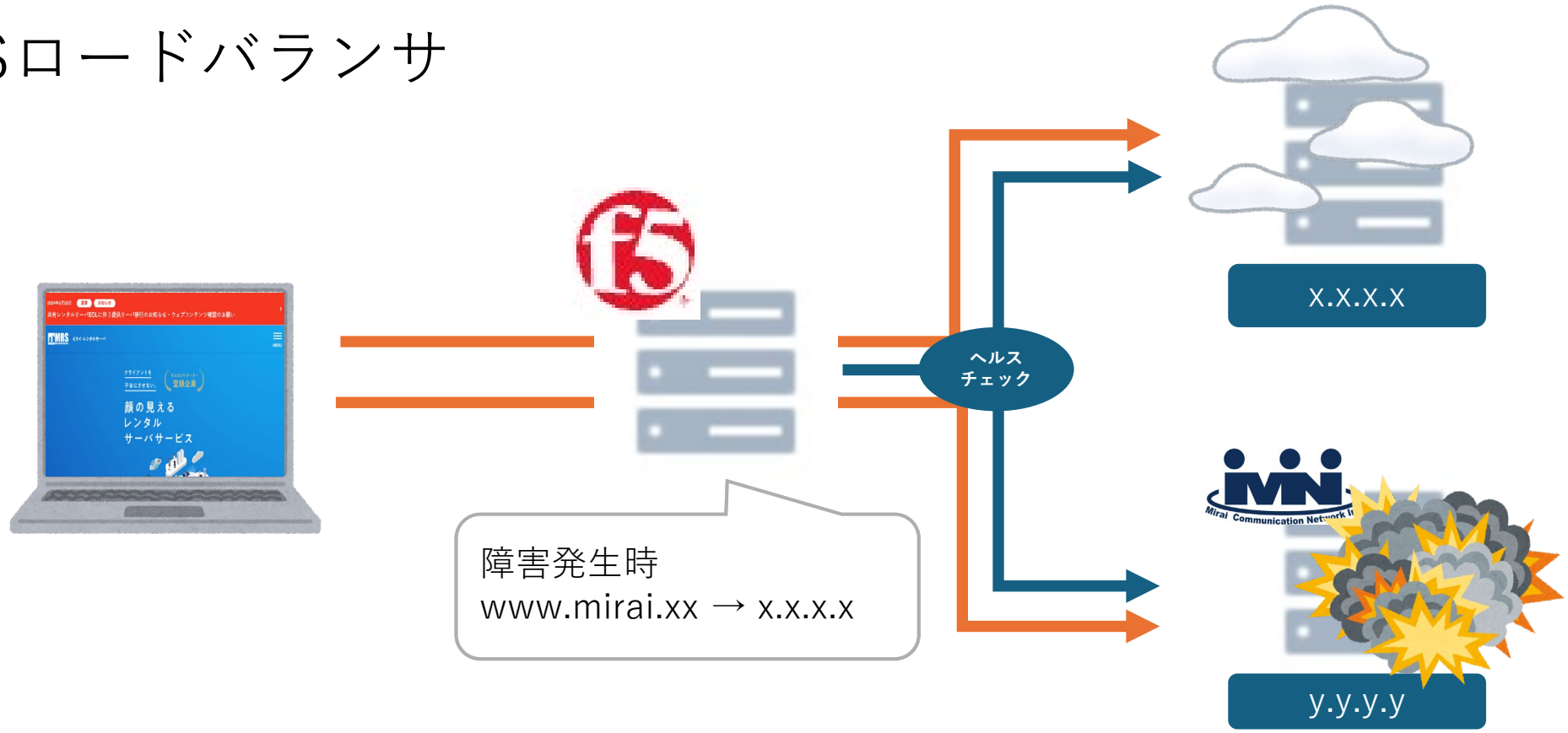
- BIND形式でのゾーン情報の
  エクスポート

→リクエスト中



今後はこんな機能も使っていきたい

- DNSロードバランサ



平常時は通信量での課金がないミライネットのWebサーバのIPアドレスを返し、
障害発生時はクラウドサーバのIPアドレスを返す

まとめ

- 権威DNSサーバの自前運用は限界に来ていると感じる
  悲しいけれど、DNSは、自分たちで、OSSだけで、何とか頑張る時代ではなくなってしまった・・・技術力もリソースも体力も必要！
- ミライネットでは「導入のしやすさ」「コストメリット」でDistributed Cloud DNSを選択
- 何を基準に選んだらいいのか…という時は、DNSOPS.jpの権威DNSサービス調査報告書をぜひ参考に
- 「買ったら終わり」ではない、F5のエンジニアのきめ細かいサポート
- 1ユーザとして今後も積極的にフィードバックしていきたい


Mirai Communication Network Inc.


App
World
2024