

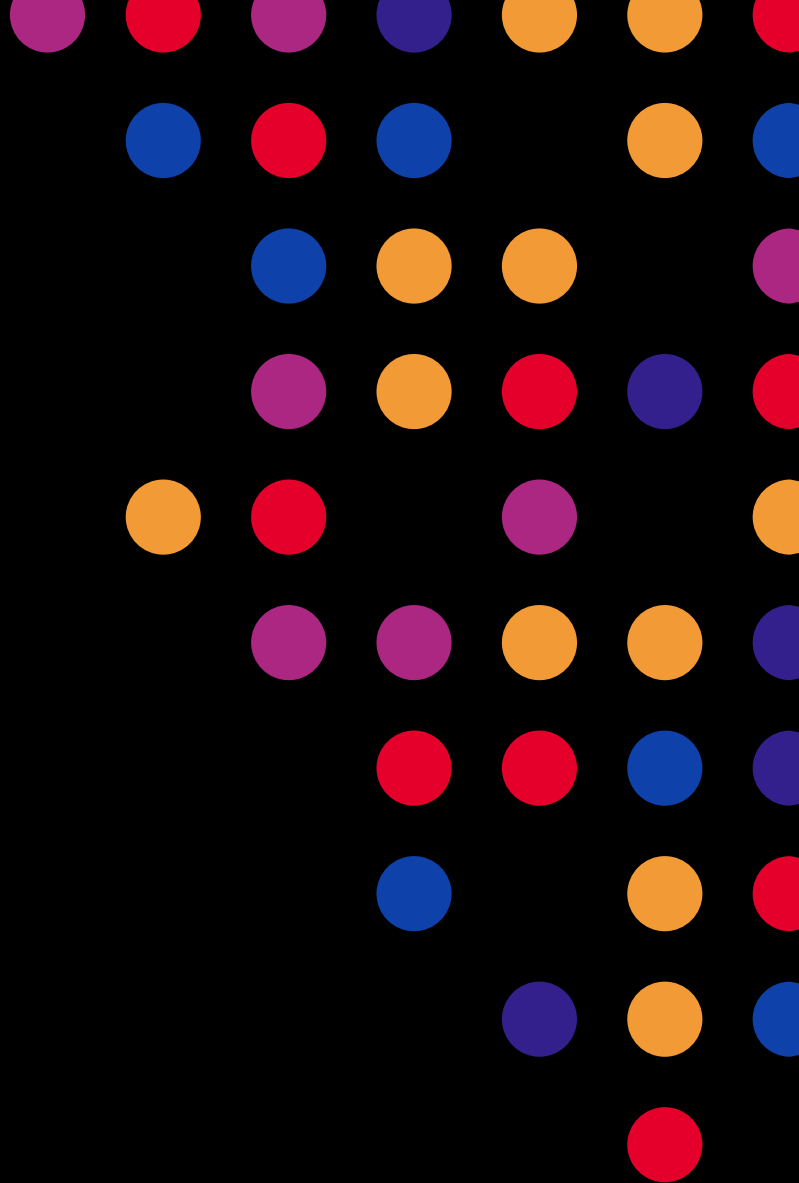


【DNS】 少人数での自前運用から Distributed Cloud DNSに 切り替えることにした話

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



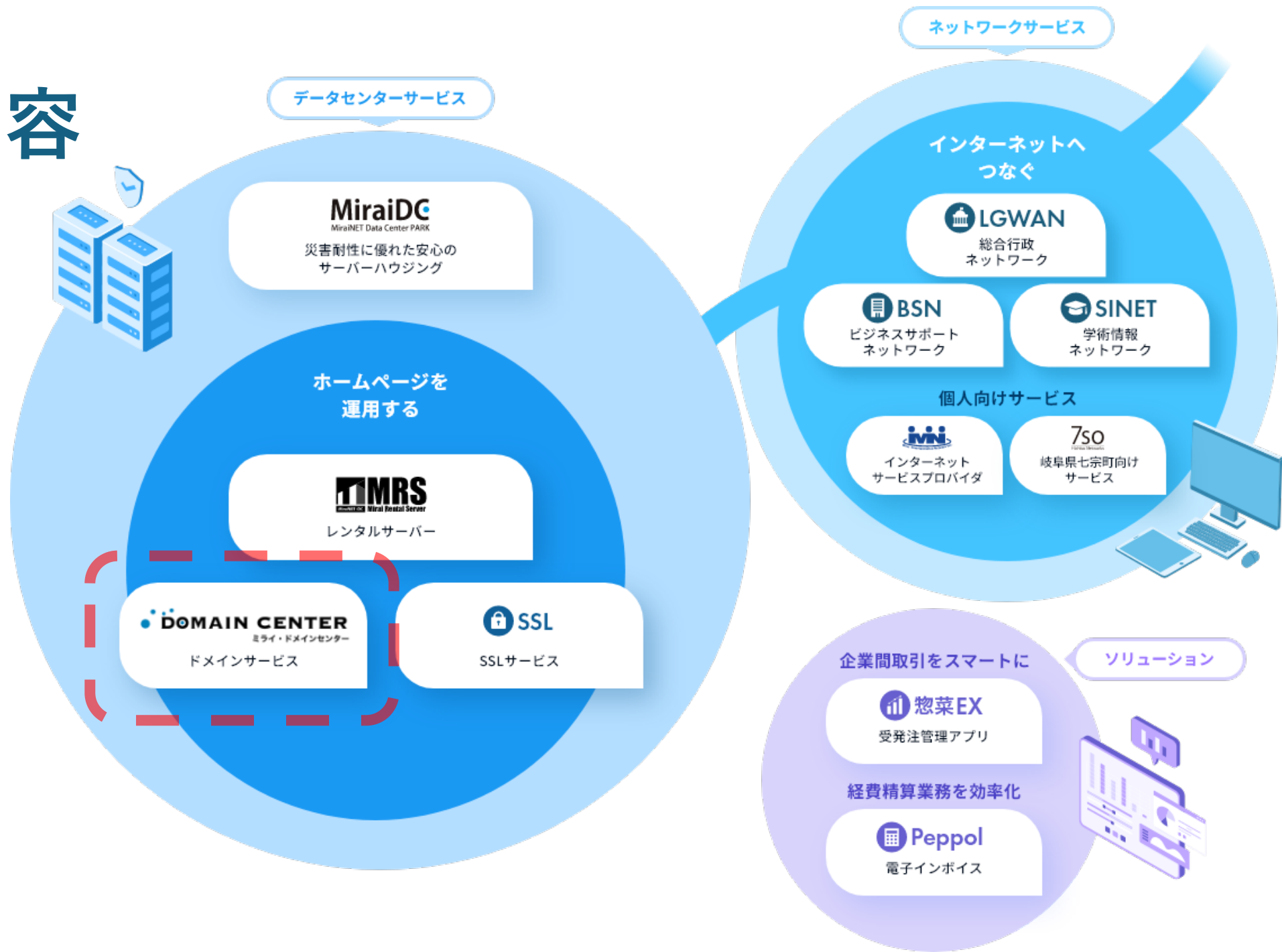
会社紹介

- 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

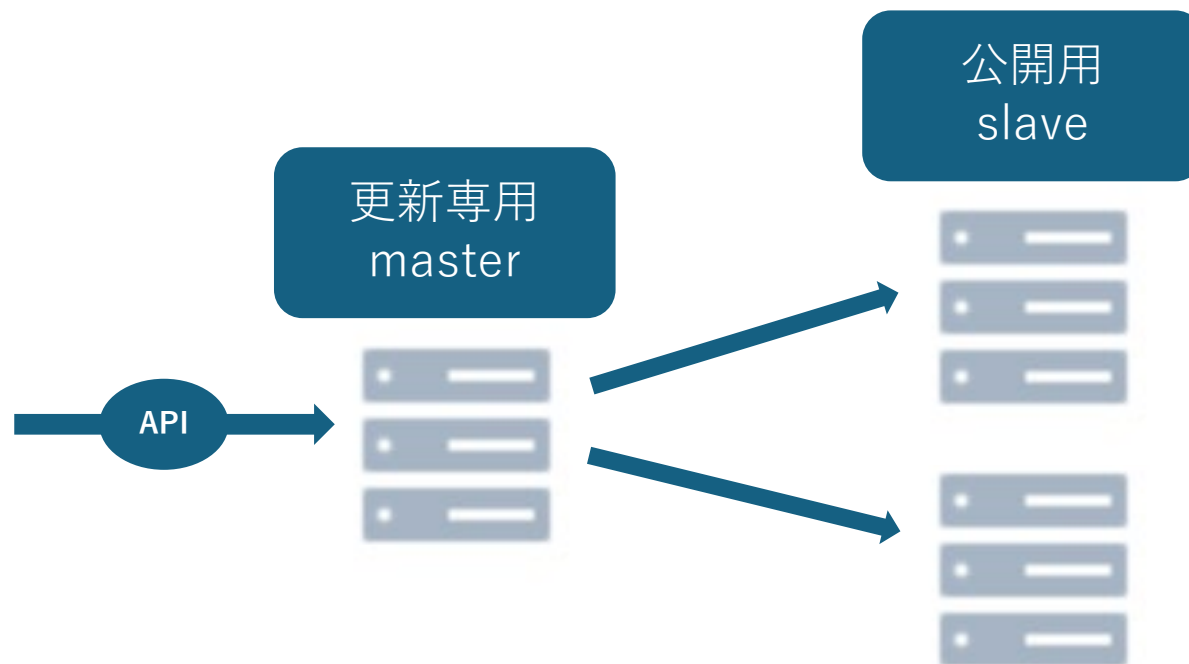
事業内容



既存システムの課題

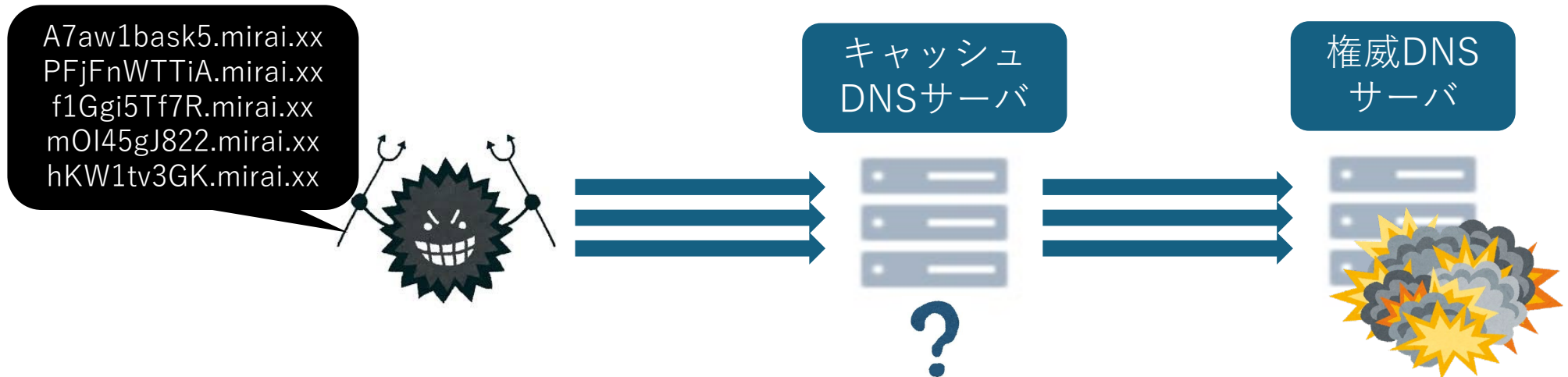
既存の権威DNSサーバの構成

- 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

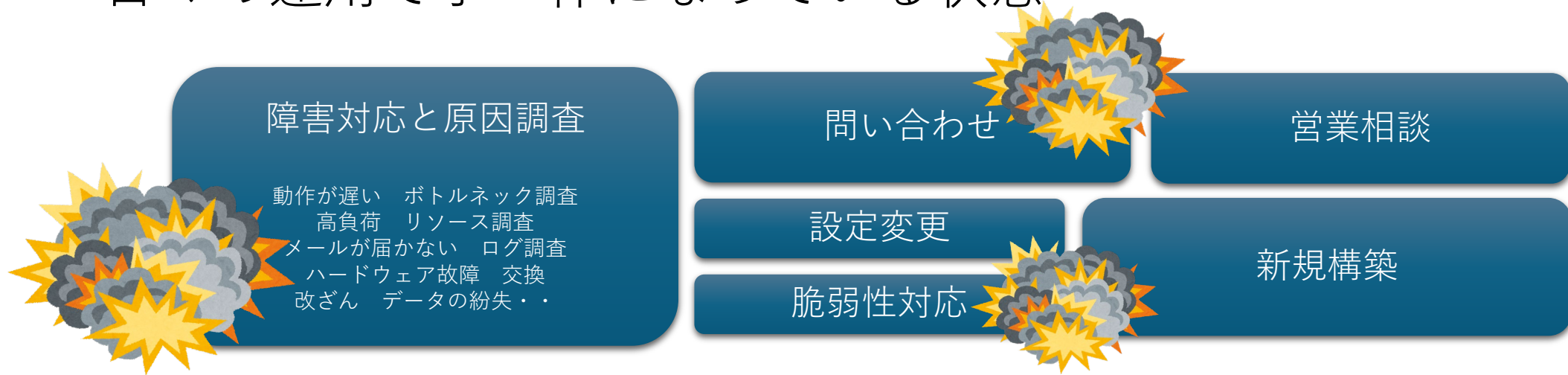
攻撃への対処

- 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
- 実際は場当たりの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

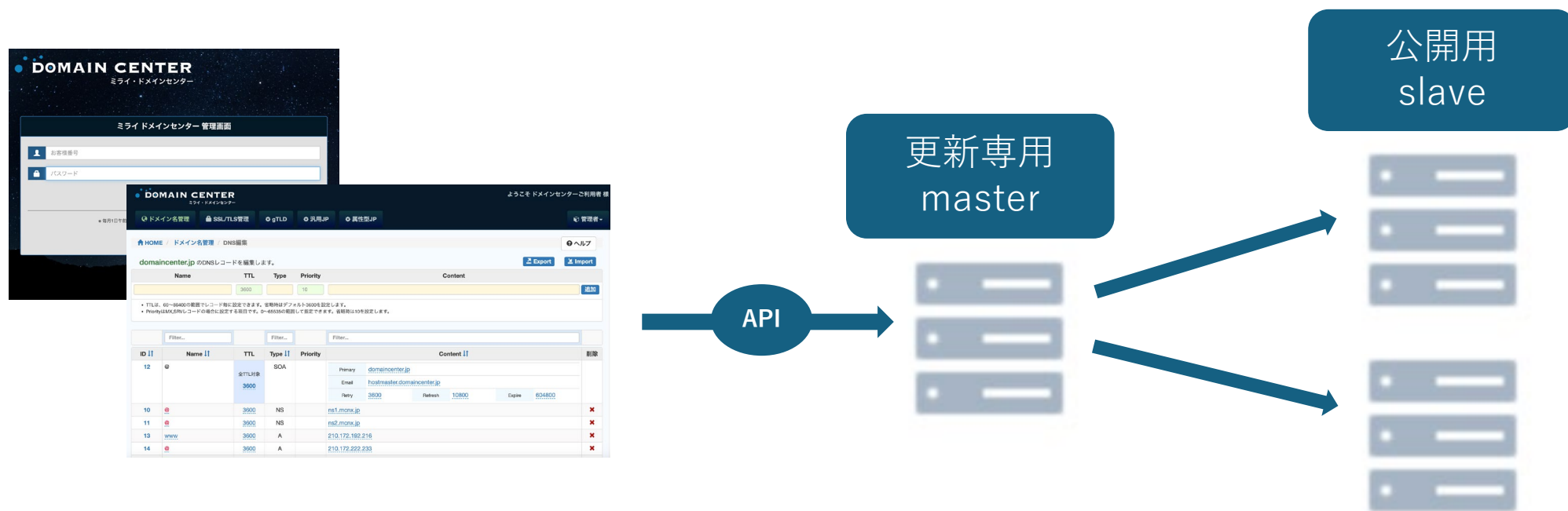
- ホスティングサーバの構築・運用を行うメンバーは9名
DNSの専門チームはなし
- 日々の運用で手一杯になっている状態・・・



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



顧客向けのインター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



権威DNSサービス調査

概要

インターネットサービスの多様化により、サービス情報を提供する汎用データベースとしてDNSの役割が増加しています。それにともない新しいリソースレコードの定義や、既存リソースレコード(特にTXTレコード)のユースケース追加などが行われています。

その一方で、一般的な組織の権威DNSサーバ運用者(ゾーン管理者)はDNSプロトコルや新しいインターネットサービスの専門家ではないため、すべてのリソースレコードを理解し正しく設定できることは期待できません。また、昨今の状況下では、設定ミスや外部からの大量クエリの集中によってサービス障害が発生する原因となり得るため、一般的な組織における権威DNSサーバの自前運用は多大な困難を伴うものになってきています。

このような状況の変化にともない、組織のシステム管理部門やサービス提供部門が、それぞれの目的に沿って適切な権威DNS(自ゾーン)を運用可能とするため、国内外で提供されている代表的な権威DNSサービスの機能一覧作成が望まれています。

DNSOPS.JPでは、そのような機能一覧となることを目的として、2020年から権威DNSサービスの調査を開始しています(注)。中立な調査を行うため、各種権威DNSサービスの利用に真正面から取り組み、機能一覧に加え、現場の運用者が直面する契約から運用開始に至るまでを含む、Boot Campと呼ぶにふさわしい実体験に基づく報告を作成しています。

注：機能の優劣をつけることや、特定のサービスを推奨することは調査および結果報告の目的ではありません。

調査結果報告書

2022年4月14日版

日本DNSオペレーターズグループ

調査報告書は公開されている

権威DNSサービス仕様調査-00										
ファイル 編集 表示 挿入 表示形式 データ ツール 拡張機能 ヘルプ										
Q メニュー 100% 閲覧のみ										
B23	A	B	C	D	E	F	G	H	I	J
1										
2	事業者名			IJ	Cloudflare	Akamai	Amazon	Microsoft	Google	IBM
3	サービス名	書けるかな?		IJ DNSプラットフォームサービス	Managed DNS	Edge DNS	Route53	Azure DNS	Cloud DNS	IBM cloud DNS
4	主要な情報源			1	2	3	4	5	6	7
5	凡例			購入済み	購入済み	購入済み	購入済み	購入済み	購入済み	
6				○	?	?	○	○	○	○
7				○	?	?	○	○	○	○
8				○	Enterpriseのみ	○	○(IAMで)	○	○	?
9				○	?	○	○	○?	?	○
10				○	○	?	○	?	○	?
11				○	○	?	○	?	○	?
12										
13	(2)可用性									
14		権威サーバが地域NW的に複数展開		○	○	○	○	○	○	○
15		適切な閾値でレスポンスレートリミットが可能であること		?	○	○	?	?	?	○
16		他の権威DNSサービスとセカンダリ構成をとることが可能		○?	○(DNSSECNG)	○(DNSSEC時はShadow構成のセカンダリならいける?)	○(DNSSECはNG)	--	○(DNSSECもTransferで行けるか?)	?
17		指定した地域でサービスが利用可能であること		?	○?	○	?	?	?	?
18		SLA規定があること		○?	○	○	○	○	○	○
19		更新処理がDR構成になっていること		?	?	?	?	?	?	?
20										
21	(3)完全性									
22		バックアップの有無、頻度、保存期間		○	?	?	?	?	?	?
		DNSSECに対応していること(鍵管理が可能であること)		○	ONSEC	○?	ONSEC	--	○	?



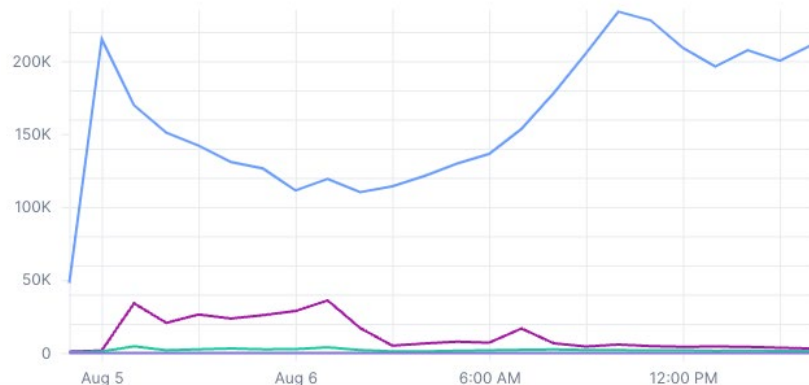
Distributed Cloud DNSを 実際に使ってみて

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

Response Type (by RCODE) ⓘ

NOERROR SERVFAIL NXDOMAIN REFUSED

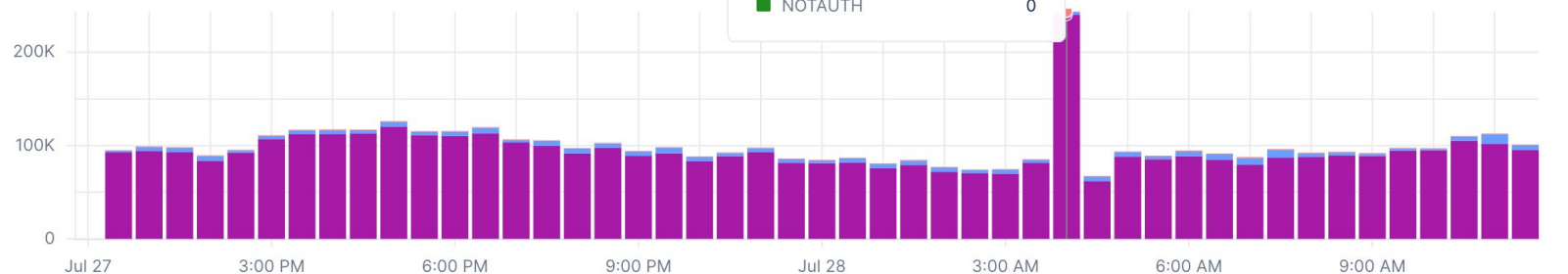


500 items

Add Filter

NOERROR SERVFAIL NXDOMAIN REFUSED FORMERR NOTAUTH

27 Jul 12:00 - 28 Jul 11:59



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

The screenshot shows a web interface for managing DNS zones. On the left, a sidebar lists configuration options for the zone 'mcnx.jp'. The main area displays 'Resource Record Sets' in a table. A blue callout box is overlaid on the table, containing the following text:

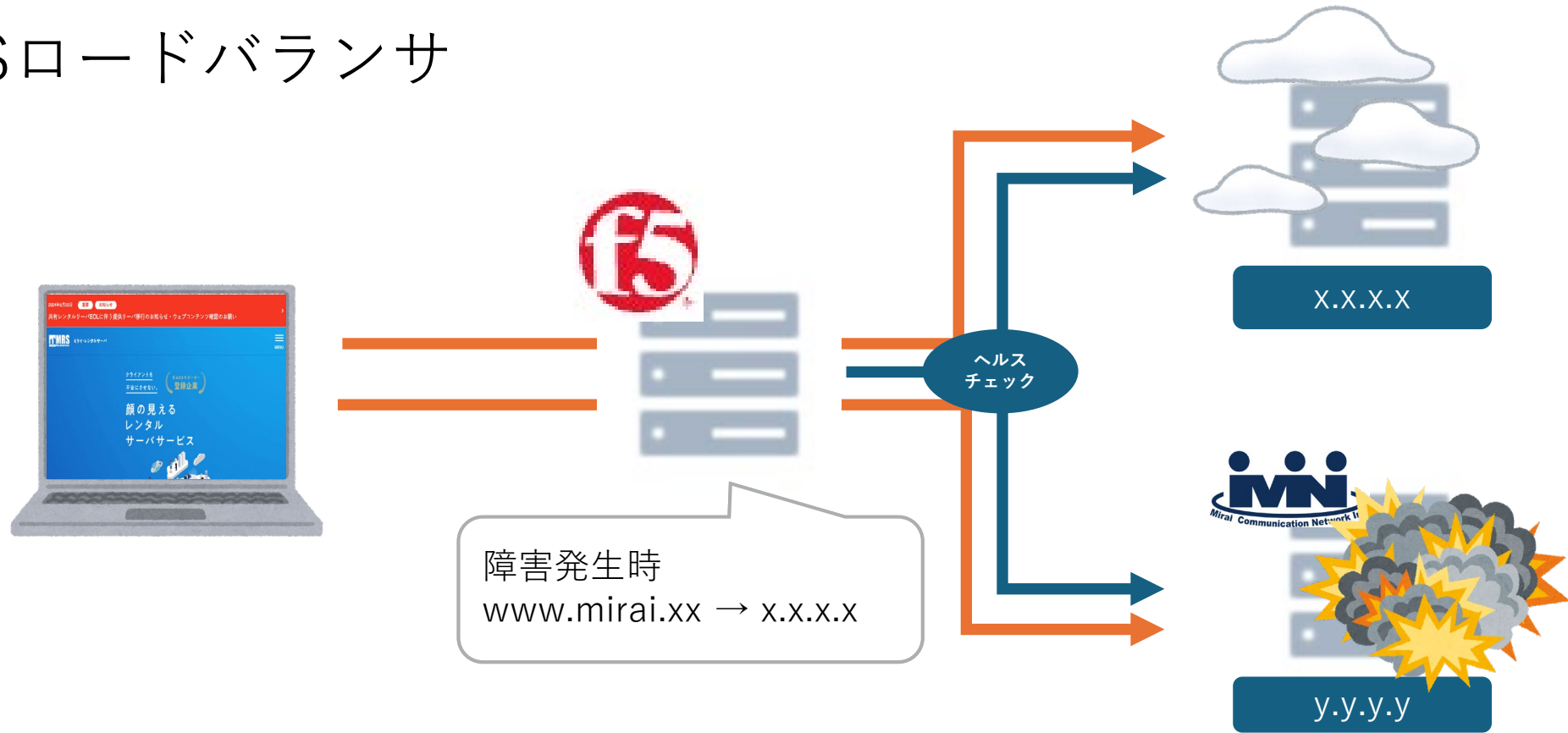
改ページが10件表示固定で
全件検索ができないので
数百レコードがあると辿り着くのが大変

Type	Record Name	Record Value(s)	TTL	Comment
A	pv504	210.172.223.216	3600	
AAAA	pv504	2407:d600:0:105:210:172:223:216	3600	
TXT	pv504	v=spf1 +ip4:210.172.223.216 ...	3597	
A	pv570	210.172.223.216	3600	
AAAA	pv570	2407:d600:0:105:210:172:223...	3600	
TXT	pv570	v=spf1 +ip4:210.172.223.216 ...	3597	
TXT	_dmarc.ov160	v=DMARC1;p=none;	3598	
TXT	_dmarc.ov174	v=DMARC1;p=none;	3598	
TXT	_dmarc.pv519	v=DMARC1;p=none;	3598	
A	demo38	210.172.223.226	3600	

Page 1 of 63

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



