DNSにおける別名ドメインの管理・運用手法

山井成良[†1] 久保武志[†2] 岡山聖彦[†3]
山外芳伸[†4] 宮下卓也[†1]

汎用 jp ドメインの運用開始にともない，新規にドメイン名を取得する組織が増加しつつある．このような組織において新規ドメイン名を従来から運用していたドメイン名の別名として利用する場合，従来の DNS の仕組みでは，サブドメイン以下の各ドメインの DNS サーバについて従来のドメインに加えて新規ドメインの設定も行う必要があるなど，管理・運用上の問題があった．そこで本稿では，別名ドメインを運用する組織において上記の問題を解決する DNS 管理・運用手法を提案する．本手法では DNS プロクシの導入によりサブドメイン以下の各ドメインに存在する DNS サーバやメールサーバの設定を変更せずに別名ドメインを運用することが可能になる．

A Management and Operation Method of DNS for Alias Domain Names

Nariyoshi Yamai,[†1] Takeshi Kubo,[†2] Kiyohiko Okayama,[†3]
Yoshinobu Yamasoto[†4] and Takuya Miyashita[†1]

Since operation of general-use JP domains started, organizations registering new domain names have been increasing. In case that new domain names are used as aliases of the existing domain name in such organizations, the current DNS mechanism has some problems in operation and management such that all DNS servers for the subdomains or the lower domains have to be configured for the new domains in addition to the existing domain. In this paper, to solve these problems, we propose a management and operation method of DNS for organization operating alias domains. By introducing a DNS proxy, this method allows alias domains to be operated without modifying the configurations of the DNS servers and the mail servers in the subdomains or the lower domains.

1. はじめに

最近，.com，.org などの従来の gTLD（generic Top Level Domain）に加えて .biz，.info など 7 つの gTLD の新設が決定されたり[1]，JP ドメインにおいても従来の属性型あるいは地域型のドメインに加えて汎用 JP ドメインのサービスが開始されたり[2] するなど，ドメイン名を取り巻く環境が大きく変わりつつある．特に平成 13 年 4 月より開始された汎用 JP ドメイン名は，(1) 日本語のドメイン名の登録が可能，(2) 複数のドメイン名が登録可能などの特徴を有するため，多くの組織が従来のドメイン名（以下，既存ドメイン名と呼ぶ）に加えて，日本語のドメインを含めた新規のドメイン名（以下，新規ドメイン名と呼ぶ）を取得している．たとえば，我々が所属する岡山大学においても，既存ドメインである okayama-u.ac.jp に加えて 5 つの汎用 JP ドメイン（okayama-u.jp，okadai.jp，岡山大学 .jp，岡山大 .jp，岡大 .jp）を取得している．

取得した新規ドメイン名には種々の用途が考えられるが，主要な用途として，既存ドメイン名の別名（別名ドメイン）としての利用があげられる．これは，たとえば www.okayama-u.ac.jp の代わりに www.okadai.jp が利用できることを意味し，これによりドメイン名やホスト名が簡略化されてその入力が容易になったり，利用者がドメイン名やホスト名を連想しやすくなったりするなどの効果が期待できる．そこで以下では別名ドメインの管理・運用について議論する．

ところで，現在インターネット上でドメイン名の管理・運用に用いられている DNS（Domain Name System）の仕組みでは，計算機名には別名の設定が可能

†1 岡山大学総合情報処理センター
Computer Center, Okayama University
†2 岡山大学大学院自然科学研究科
Graduate School of Natural Science and Technology, Okayama University
†3 岡山大学工学部
Faculty of Engineering, Okayama University
†4 株式会社ジークス
ZYYX Inc.

であるが，ドメイン名には別名の設定は許されていない．そのため，新規ドメインを既存ドメインの別名として利用するには，組織内のすべてのDNSサーバにおいて新規ドメインの設定を個別に行う方法が一般的に用いられてきた．しかし，サブドメインやさらに下位のドメイン（以下ではこれらをまとめて子孫ドメインと呼ぶ）の数が多い組織に対して適用する場合，この方法は，設定が必要なDNSサーバの数が多くなり，管理コストが大きくなる点が問題となる．このような組織の多くでは，子孫ドメインの管理が複数の管理者により独立して行われ，すべての管理者が協調して新規ドメインに対する設定を行う必要が生じるため，1人の管理者が集中して管理する場合と比べると全体の管理コストはさらに大きくなる．また，電子メールでも，たとえば `user@cc.okayama-u.ac.jp` の代わりに `user@cc.okadai.jp` を利用できるなど，別名ドメインを含むアドレスを既存ドメインを含むアドレスの代わりに利用できるようにするためには，DNSサーバと同様にメールサーバにおいても組織内のすべてのサーバで設定変更が必要となる．

DNSサーバの管理を省力化するための研究は数多く行われており，たとえば文献3)などがあげられる．しかし，従来の研究のほとんどは1つのドメイン空間の管理省力化を目的としており，別名ドメイン空間の管理には適用できない．たとえこれらを別名ドメイン空間を管理できるように拡張したとしても，導入時に子孫ドメインごとにDNSサーバの設定変更が必要となる点は変わらず，管理コストの大きな削減にはつながらない．

そこで本稿ではDNSプロクシを導入して上記の問題を解決する手法を提案する．本手法では，DNSの問合せ/応答メッセージを受け取るとその中に含まれるドメイン名を変換して中継する機能をDNSプロクシに持たせており，これにより組織内のDNSサーバを設定変更せずに別名ドメイン名を管理・運用することが可能となる．また，同様にDNSの応答メッセージにMXレコードを書き換えたり追加したりする機能をDNSプロクシに持たせており，これにより組織内のメールサーバを設定変更せずに別名ドメインに属するアドレスを利用することが可能となる．

2. 従来の別名ドメイン管理・運用手法と問題点

新規ドメイン名を既存ドメイン名の別名として利用する場合，従来の技術を用いたドメイン管理・運用手法がいくつか考えられる．しかし，特に多数の子孫ドメインが存在し，それらの管理が独立して行われるような大規模な組織においては，従来の手法は管理コストの面で問題がある．

本章ではこれらの手法を示し，また大規模な組織に適用した場合の問題点を明らかにする．

2.1 各DNSサーバでの設定変更

別名ドメインを管理・運用する手法として最も一般的であるのは，これを独立したドメインと見なし，組織内のすべてのDNSサーバにおいて新規ドメインの設定を個別に行う手法である．この場合，最もよく用いられているDNSサーバであるBIND[4]では，複数のドメイン間でゾーンファイルを共用することにより，各DNSサーバの設定をある程度簡略化することが可能である．

しかし，この手法では運用開始時だけでなく，別名ドメインの追加・削除・変更☆時にも組織内のすべてのDNSサーバの設定を変更する必要がある．同様に，電子メールにおいても別名ドメインを含むアドレスを利用できるようにするには，組織内のすべてのメールサーバの設定を変更する必要が生じる．たとえば，1章で述べた例では，`cc.okayama-u.ac.jp` に対応するメールサーバにおいて `user@cc.okayama-u.ac.jp` 宛だけでなく `user@cc.okadai.jp` 宛の電子メールも受け取るように設定を変更しなければならない．

以上のように，この手法は組織内のすべてのDNSサーバおよびメールサーバの設定変更をともなうため，これらのサーバの設置台数が多い大規模な組織では，管理コストが膨大となる点が問題となる．特に大学などの教育機関では，文系の学部など必ずしも経験豊富な管理者がいるとは限らない下部組織が独自にこれらのサーバを設置・運用している場合があり，その場合にはこの手法の採用は困難である．

2.2 1つのDNSサーバでの集中管理

別名ドメインを管理・運用する別の方法として，組織内にDNSサーバを1台用意して集中的に別名ドメインの管理・運用を行う手法が考えられる．この手法では，別名ドメイン用DNSサーバはすべての子孫ドメインのゾーン情報を収集して別名ドメイン用にNSレコードなどの一部のリソースレコードを書き換えたうえで再利用し，別名ドメインに関するすべての名前解決を行うようにする．

この手法の利点は，別名ドメインの追加・削除・変更時にも別名ドメイン用のDNSサーバについてのみ設定を変更すればよく，組織内の他のDNSサーバの

☆ 多言語ドメイン名の正規化方式および文字エンコーディング方式の標準化にともない，日本語のドメインについてはASCII表記のドメイン名の変更が予定されている[5]．

設定は変更する必要がなくなる点にある．また，別名ドメインを含むアドレスの利用についても，次章で提案する手法と同様に MX レコードを書き換えることにより子孫ドメインのメールサーバの設定変更を不要にすることが可能である．

しかし，この手法は DNS の運用ポリシーによっては適用できない場合がある．すなわち，この手法では組織内の各 DNS サーバが新規ドメイン用 DNS サーバに対してゾーン情報の転送を許可していることが適用の前提となっているため，この転送を許可しないような運用ポリシー（たとえばセカンダリ DNS サーバに対してのみゾーン転送を許可するような運用ポリシー）を採用している組織では適用できない．この場合，たとえ新規ドメイン用 DNS サーバへの転送を許可するように運用ポリシーを変更したとしても，実際にゾーン転送を行うには各 DNS サーバの設定を変更しなければならず，この手法の導入にはかなりの管理コストが必要になると思われる．このような運用ポリシーは，セキュリティ上の理由により標準的に採用されているため，この手法の導入にともなう管理コストは多くの組織で問題となりうる．

なお，すべての子孫ドメインに対する共通のセカンダリ DNS サーバが組織内のどこかで運用されている場合には，各子孫ドメインの DNS サーバの設定を変更しなくても，このセカンダリ DNS サーバからすべての子孫ドメインのゾーン情報を入手することにより，この手法を適用できる．しかし，特に既存ドメインの階層が深いような規模の大きな組織は，必ずしもこの場合に該当するとは限らず，この手法はすべての組織に適用することができない．

3. DNS プロクシによる複数ドメインの管理・運用手法

3.1 提案手法の構成と動作

前章で述べたように，従来の別名ドメイン管理・運用手法はいずれも管理コストが大きく，規模が大きい組織に適用する場合には問題となりうる．そこで，本稿では，DNS プロクシの導入により，別名ドメインと既存ドメインとの間で DNS の問合せ/応答メッセージを変換する手法を提案する．これにより，任意の組織において管理コストを抑えながら別名ドメインを管理・運用することが可能になる．

以下では，`example.co.jp` の別名ドメインとして `example.jp` を運用する場合を例にとり議論する．なお，以下の議論では，簡単化のためにリソースレコードの種類として A，MX，CNAME，NS，SOA だけを考慮し，その他の種類のリソースレコードは考慮しないものとする．また，別名ドメインに対するセカンダリ DNS サーバはないものとする．ただし，本手法はセカンダリ DNS サーバを考慮した場合にも容易に対応できる．

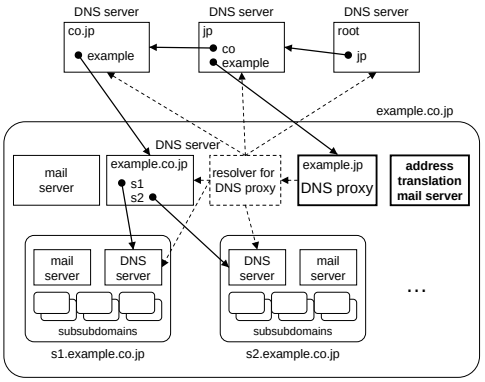

図 1 提案手法の構成
Fig. 1 A structure of the proposed method.

まず，本手法の構成を**図 1** に示す．この図において，細実線の長方形は既存のサーバを，太実線の長方形は新たに導入されたサーバを示し，また破線の長方形は不要な場合があるサーバを示す．さらに，実線の矢印は DNS における NS レコードによる参照を示し，また破線の矢印は DNS プロクシが発信する DNS 問合せメッセージの流れを示す．

この図に示すように，本手法では別名ドメインに対する DNS の問合せ/応答メッセージを変換して中継する DNS プロクシ（DNS proxy）と，別名ドメインに属するアドレスを既存ドメインのものに変換する役割を果たすメールサーバ（以下，アドレス変換メールサーバ（address translation mail server）と呼ぶ）があり，これらのサーバが既存ドメイン用の DNS サーバやメールサーバと協調して動作することにより別名ドメインを利用できる．この図には DNS プロクシ用のリゾルバ（resolver for DNS proxy）が示されているが，これは既存ドメインの名前解決に用いられるもので，任意の DNS サーバを利用することができる．したがって，たとえば `example.co.jp` のプライマリ DNS サーバでもかまわないし，あるいは DNS プロクシ自身が既存ドメインの名前解決を行ってもよい．

次に，DNS プロクシの動作の概略について述べる（**図 2** 参照）．なお，アドレス変換メールサーバの動作については後述する．

DNS プロクシは別名ドメインおよびそのすべての子孫ドメインのプライマリ DNS として動作し，上位ドメイン（図 1 の例では `jp`）の DNS サーバから直接

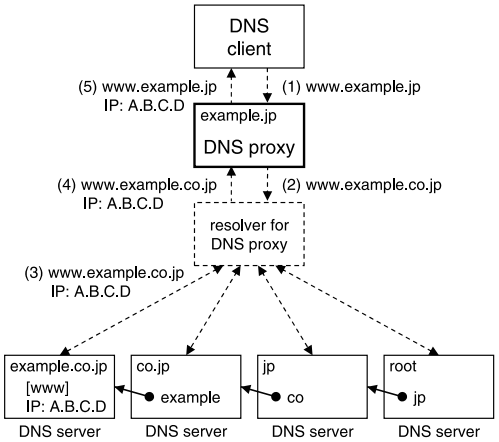

図 2 提案手法の動作例
Fig. 2 A sample action sequence of the proposed method.

参照される．このため，別名ドメインに関するすべての DNS 問合せメッセージは最終的に DNS プロクシに送られることになる（図 2 (1)）．DNS プロクシは別名ドメインに関する DNS 問合せメッセージを受け取ると，これを既存ドメインに関する DNS 問合せメッセージに変換して DNS プロクシ用のリゾルバに送る（同 (2)）．リゾルバは DNS 問合せメッセージを受け取ると，他の DNS サーバに問い合わせて既存ドメインの名前解決を行い（同 (3)），その結果を DNS プロクシに返す（同 (4)）．DNS プロクシはこれを別名ドメインに関する DNS 応答メッセージに変換して，問合せ元に返す（同 (5)）．

以上の動作により，本手法は既存ドメインの構造，組織内における DNS サーバの管理方法やプログラムの種類，あるいは管理ポリシーに依存せず，広範囲に適用することが可能となる．また，DNS プロクシおよびアドレス変換メールサーバで必要な設定は，前者は新規ドメイン名，既存ドメイン名およびアドレス変換メールサーバ名の 3 つ，後者は新規ドメイン名，既存ドメイン名の 2 つだけであり，管理コストを大幅に削減することができる．

3.2 DNS メッセージの書換え

DNS メッセージは文献 6) に示されるように，問合せ，応答とも Header，Question，Answer，Authority，および Additional の 5 つのセクションから構成される．DNS プロクシは受け取ったメッセージのすべてのセクションを調べ，必要に応じてレコードの書換えを行う．以下では，A レコードの問合せ/応答，MX レコードの問合せ/応答，およびその他のレコードの問合せ/応答の各場合について，DNS プロクシにおけるメッセージの書換え方法を示す．

[Question section]	⇒	[Question section]
host.example.jp		host.example.co.jp

図 3 問合せメッセージの書換え
Fig. 3 Rewriting of a query message.

[Question section]		[Question section]
www.example.co.jp		www.example.jp
[Answer section]		[Answer section]
www.example.co.jp		www.example.jp
IP: A.B.C.D		IP: A.B.C.D
[Authority section]	⇒	[Authority section]
example.co.jp		example.jp
NS: dns.example.co.jp		NS: dns.example.jp
[Additional section]		[Additional section]
dns.example.co.jp		dns.example.jp
IP: E.F.G.H		IP: E.F.G.H

図 4 応答メッセージの誤った書換え例
Fig. 4 Wrong rewriting of a reply message.

3.2.1 A レコードの問合せ/応答における書換え

まず，電子メールを含むほとんどすべてのサービスで用いられる，A レコードの問合せ/応答についてメッセージの書換え方法を示す．

問合せメッセージは Header および Question の 2 つのセクションにだけ有効なデータが格納されており，その他のセクションは空である．A レコードの問合せメッセージを受け取ると，DNS プロクシはまず Question セクションを調べ，その中の QNAME フィールドに書換えの対象となる別名ドメインが含まれていれば，**図 3** のようにその部分を既存ドメインに書き換える．その後，DNS プロクシは書き換えたメッセージを通常の問合せと同様の手順で名前解決を行う．このとき，DNS プロクシは別名ドメインおよびその子孫ドメインに関するプライマリ DNS サーバとして振る舞うため，A レコードを入手するまで再帰モードで問合せを行う．

書き換えた問合せに対する A レコードを得ると，DNS プロクシはこの A レコードを含んだ応答メッセージを作成して問合せ元に送信する．このとき，DNS プロクシは Question セクションや Answer セクション（CNAME レコード）に含まれる既存ドメイン名を問合せメッセージに含まれていた別名ドメイン名に書き換えるが，ここで**図 4** のように Authority セクションに含まれる既存ドメイン名を単純に別名ドメインに書き換えると，問題が生じることに注意する．すなわち，図 4 のような応答メッセージでは，`example.jp` ドメインの管理権限を持っているのは，DNS プロクシではなく `dns.example.jp` であると解釈されるため，場合によっては `example.co.jp` ドメインの管理権限を有する `dns.example.co.jp`（IP アドレス E.F.G.H）に

[Question section]		[Question section]
www.example.co.jp		www.example.jp
[Answer section]		[Answer section]
www.example.co.jp		www.example.jp
IP: A.B.C.D		IP: A.B.C.D
[Authority section]	⇒	[Authority section]
example.co.jp		example.jp
NS: dns.example.co.jp		NS: proxy.example.jp
[Additional section]		[Additional section]
dns.example.co.jp		proxy.example.jp
IP: E.F.G.H		IP: J.K.L.M

図 5 応答メッセージの正しい書換え例
Fig. 5 Right rewriting of a reply message.

www.example.jp の A レコードを問い合わせるメッセージが送られ，結果としてエラーとなる可能性がある．そこで，DNS プロクシは**図 5** のように Authority セクションの NS レコードを DNS プロクシ（proxy.example.jp）自身が管理権限を有していると見えるように書き換え，また Additional フィールドには DNS プロクシ自身の A レコード（J.K.L.M）を記述するようにする．

3.2.2 MX レコードの問合せ/応答における書換え

MX レコードの問合せは主に電子メールの配送先を決定する際に発生する．このとき，問合せメッセージの書換えは A レコードの場合と同じ要領でよいが，応答メッセージの書換えには注意を要する．すなわち，A レコードの場合と同様に CNAME レコードに含まれる既存ドメインは問合せメッセージ中に含まれていた別名ドメインに書き換えてもよいが，MX レコード中に含まれる既存ドメイン名は単に問合せメッセージに含まれていた別名ドメイン名に書き換えただけでは，別名ドメイン名を含むアドレス宛の電子メールがこれを受理できないメールサーバに直接配送されることになる．そこで，DNS プロクシでは**図 6** に示すように，本来の応答メッセージに含まれていた MX レコード全体を破棄し，代わりにアドレス変換メールサーバ（tr.example.jp）を指す MX レコードを追加するようにする．同様の理由により，本来の応答メッセージに MX レコードが含まれていない場合にも，アドレス変換メールサーバを指す MX レコードを追加する．また，これらの変更に合わせて，Additional セクションでも MX レコードに対応する A レコードをアドレス変換メールサーバの IP アドレス（R.S.T.U）に書き換える．

このような書換えを行った場合における，別名ドメイン宛（たとえば user@example.jp 宛）の電子メールの配送手順を**図 7** に示す．まず，発信元のメールサーバは身近な DNS クライアントを介して example.jp の MX レコードを問い合わせる．この問合せは最終的には DNS プロクシが受け取る（図 7 (1)）．次に DNS プロクシは受け取ったメッセージを既存ドメイン example.co.jp の MX レコードに関する問合せメッセージに変換して，DNS プロクシ用のリゾルバに送る（同 (2)）．リゾルバは DNS 問合せメッセージを受け取ると，他の DNS サーバに問い合わせて名前解決を行い，その結果を DNS プロクシに返す（同 (3)）．DNS プロクシは応答メッセージに含まれる MX レコードをアドレス変換メールサーバ tr.example.jp に書き換え，問合せ元に返す（同 (4)）．この結果に従い，発信元メールサーバは user@example.jp 宛の電子メールをアドレス変換メールサーバに送る（同 (5)）．アドレス変換メールサーバはこの電子メールの宛先を user@example.co.jp に変換した後，本来の配送先である mx.example.co.jp に送信する（同 (6)）．

以上の動作により，本手法では組織内のメールサーバの設定を変更することなく別名ドメイン宛の電子メールを処理することが可能である．

[Question section]		[Question section]
example.co.jp		example.jp
[Answer section]		[Answer section]
example.co.jp		example.jp
MX: mx.example.co.jp		MX: tr.example.jp
example.co.jp		
MX: mx2.example.co.jp		
[Authority section]		[Authority section]
example.co.jp	⇒	example.jp
NS: dns.example.co.jp		NS: proxy.example.jp
[Additional section]		[Additional section]
dns.example.co.jp		proxy.example.jp
IP: A.B.C.D		IP: N.O.P.Q
mx.example.co.jp		tr.example.jp
IP: E.F.G.H		IP: R.S.T.U
mx.example.co.jp		
IP: J.K.L.M		

図 6 MX レコードの問合せに対する応答メッセージの書換え例
Fig. 6 Rewriting of a reply message for MX record query.

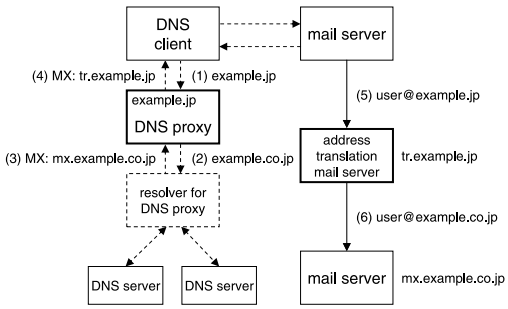

図 7 電子メールの配送手順例
Fig. 7 A sample sequence of e-mail delivery.

3.2.3 その他のレコードの問合せ/応答における書換え

その他の種類のレコードにはCNAME，NS，SOAがある．これらのレコードの問合せメッセージはAレコードの場合と同様に書き換えればよい．また，応答メッセージについても，CNAMEおよびSOAレコードに関するものは，Aレコードの場合と同様の書換えでよいが，NSレコードについては注意が必要となる．すなわち，NSレコードが1つ以上含まれていれば，DNSプロクシがプライマリDNSサーバであると見えるように書き換える必要がある．この場合，これらの変更に合わせて，Additionalセクションでも NSレコードに対応するAレコードをDNSプロクシ自身のIPアドレスに書き換えるようにする．

このほかに，QTYPEがANYである問合せメッセージを用いてすべてのレコードを問い合わせる場合がある．この場合には，MXレコードおよびNSレコードの書換え処理を両方とも行えばよい．

3.3 アドレス変換メールサーバの設定

アドレス変換メールサーバはアドレスに含まれる別名ドメインを既存ドメインに変換して中継する役割を果たす．このような変換を行う機能はsendmail[7]などのMTAには備わっており，たとえばsendmailの設定ファイル作成プログラムであるCF[8]を用いて容易に設定を行うことができる．なお，この設定では，別名ドメイン宛の電子メールの中継を不正な中継と見なして配送拒否しないように注意する必要がある．

4. DNSプロクシの実装と性能評価

4.1 DNSプロクシの実装

前章で述べた手法に基づき，我々はFreeBSD4.1-Release上でDNSプロクシを試作した．プログラムの開発はC言語で行い，プログラムサイズは約3,000行である．

本プログラムは以下のように動作する．

起動時に本プログラムは設定ファイルから既存ドメイン名，1つ以上の別名ドメイン名，ならびにアドレス変換メールサーバ名を読み込み，メッセージの到着を待つ．ここで問合せメッセージを受信すると，本プログラムはその中に含まれるID番号と問合せ元IPアドレスを記録し，前章で説明したようにメッセージを書き換えてDNSプロクシ用のDNSサーバ☆に送出する．また，これに対する応答メッセージを受信すると，本プログラムはこれを書き換えてID番号に対応する問合せ元に送出する．

☆ `/etc/resolv.conf` ファイルで指定されるシステム標準のもの．

4.2 動作確認

次に，`okayama-u.ac.jp`ドメインに対応する別名ドメインとして`test.okadai.jp`を設定してDNSプロクシの試験運用を行った．この試験運用では，DNSプロクシを計算機`router2.cc.okayama-u.ac.jp`[150.46.42.144]上で動作させ，またアドレス変換サーバとして計算機`jedi.cc.okayama-u.ac.jp`[150.46.42.93]を指定した．

`scalar.cc.test.okadai.jp`を解決する場合の動作例を**図8**に示す．この図において，5〜17行目は`scalar.cc.okayama-u.ac.jp`のすべてのレコードを問い合わせた結果であり，23〜30行目は`scalar.cc.test.okadai.jp`のすべてのレコードを問い合わせた結果である．このうち，24，25行目はそれぞれ`scalar.cc.test.okadai.jp`のMXレコードおよびAレコードを表すが，指定したアドレス変換サーバ`jedi.cc.test.okadai.jp`（`jedi.cc.okayama-u.ac.jp`と同一）および`scalar.cc.okayama-u.ac.jp`のIPアドレス[150.46.30.11]が正しく返されていることが分かる．また，28行目はAuthorityセクションを表すが，この行で示されているNSレコードもDNSプロクシ自身を指すように正しく変換されていることが分かる．

また，同様の環境において，別名ドメイン宛の電子メールが正しく配送されるかどうかを確認するための実験を行った．この実験で受信したメッセージのヘッダを**図9**に示す．6行目および9行目に示すように発信時の宛先は`yamai@cc.test.okadai.jp`であったが，3行目に示すようにアドレス変換メールサーバ`jedi.cc.okayama-u.ac.jp`で既存ドメインのアドレス`yamai@cc.okayama-u.ac.jp`に変換されて正しく配送されていることが分かる．

このほか，WWW，telnetなどのアプリケーションにおいて別名ドメイン名を利用した結果，調査した範囲内では問題なく利用できることを確認した．

これらの結果から，本手法は機能面では有効であることが確認されたといえる．

なお，上記の動作試験では確認できなかったが，WWWにおけるvirtual host機能[9]のように，一部のサービスにおいては本手法が有効でない場合があることが判明している．これについては4.4節で議論する．

4.3 性能評価

本手法ではDNSプロクシが別名ドメインのプライマリDNSサーバとして振る舞うため，別名ドメインに関するすべての問合せがDNSプロクシを経由し，

```
% nslookup -query=any scalar.cc.okayama-u.ac.jp.
Server:  ccgwews2.okayama-u.ac.jp
Address:  150.46.44.3

scalar.cc.okayama-u.ac.jp   preference = 20, mail exchanger = scalar.cc.okayama-u.ac.jp
scalar.cc.okayama-u.ac.jp   preference = 900, mail exchanger = ccews2.cc.okayama-u.ac.jp
scalar.cc.okayama-u.ac.jp   internet address = 150.46.30.11
cc.okayama-u.ac.jp  nameserver = ccgwews2.okayama-u.ac.jp
cc.okayama-u.ac.jp  nameserver = ccgwews3.okayama-u.ac.jp
cc.okayama-u.ac.jp  nameserver = mecrrsews1.hospital.okayama-u.ac.jp
cc.okayama-u.ac.jp  nameserver = mebmrsews2.med.okayama-u.ac.jp
scalar.cc.okayama-u.ac.jp   internet address = 150.46.30.11
ccews2.cc.okayama-u.ac.jp   internet address = 150.46.41.9
ccgwews2.okayama-u.ac.jp    internet address = 150.46.44.3
ccgwews3.okayama-u.ac.jp    internet address = 150.46.44.4
mecrrsews1.hospital.okayama-u.ac.jp internet address = 150.46.145.2
mebmrsews2.med.okayama-u.ac.jp  internet address = 150.46.157.14
%
% nslookup -query=any scalar.cc.test.okadai.jp.
Server:  ccgwews2.okayama-u.ac.jp
Address:  150.46.44.3

Non-authoritative answer:
scalar.cc.test.okadai.jp    preference = 9, mail exchanger = jedi.cc.test.okadai.jp
scalar.cc.test.okadai.jp    internet address = 150.46.30.11

Authoritative answers can be found from:
cc.test.okadai.jp       nameserver = router2.cc.test.okadai.jp
jedi.cc.test.okadai.jp  internet address = 150.46.42.93
router2.cc.test.okadai.jp   internet address = 150.46.42.144
```

図 8 DNS プロクシによる名前解決
Fig. 8 Name resolution example using DNS proxy.

```
Received: from jedi.cc.okayama-u.ac.jp (jedi.cc.okayama-u.ac.jp [150.46.42.93])
        by ccmail.cc.okayama-u.ac.jp (8.9.3/3.7W) with ESMTP id WAA11266
        for <yamai@cc.okayama-u.ac.jp>; Thu, 13 Sep 2001 22:35:08 +0900 (JST)
Received: from ccmail.cc.okayama-u.ac.jp (scalar.cc.okayama-u.ac.jp [150.46.30.11])
        by jedi.cc.okayama-u.ac.jp (8.9.3/3.7W) with ESMTP id WAA01754
        for <yamai@cc.test.okadai.jp>; Thu, 13 Sep 2001 22:35:08 +0900 (JST)
Received: (from yamai@localhost)
        by ccmail.cc.okayama-u.ac.jp (8.9.3/3.7W) id WAA11261
        for yamai@cc.test.okadai.jp; Thu, 13 Sep 2001 22:35:08 +0900 (JST)
Date: Thu, 13 Sep 2001 22:35:08 +0900 (JST)
From: Nariyoshi Yamai <yamai@cc.okayama-u.ac.jp>
To: yamai@cc.test.okadai.jp
Subject: test
```

図 9 別名ドメイン宛メールのヘッダ
Fig. 9 A header of an e-mail to a user in an alias domain.

DNS プロクシの性能が問合せの応答時間に大きく影響するおそれがある．そこで，次に我々は DNS プロクシの性能評価実験を行った．

本実験では**図 10** に示すように，試作した DNS プロクシのほかに，ドメイン名の問合せをするクライアント，ドメイン `okayama-u.ac.jp` のプライマリ DNS サーバ（DNS サーバ 1）およびドメイン `in.it.okayama-u.ac.jp` のプライマリネームサーバ（DNS サーバ 2）を用いた．ここで，4.2 節と同様に，DNS プロクシでは `okayama-u.ac.jp` ドメインに対応する新規ドメイ

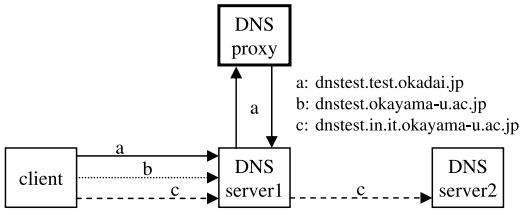

図 10 実験環境
Fig. 10 The configuration of the experiment.

ンとして `test.okadai.jp` を設定した．また，クライアントならびに DNS プロクシのリゾルバはいずれも DNS サーバ 1 となるように設定した．

この環境において，DNS プロクシのオーバヘッドを測定するために，(a) `dnstest.test.okadai.jp`（ドメイン a），(b) `dnstest.okayama-u.ac.jp`（ドメイン b）の 2 つの FQDN についてクライアント計算機から A，MX の 2 種類のレコードの問合せを 1,000 回ずつ行い，それぞれについて応答時間の最大値，最小値，平均値，標準偏差を求めて比較した．また，通常の DNS の運用における DNS 問合せメッセージの中継のオーバヘッドと比較するため，(c) `dnstest.in.it.okayama-u.ac.jp`（ドメイン c）についても同様の測定を行った．このとき，DNS サーバ 1 が DNS 問合せメッセージを確実に DNS サーバ 2 に中継するように，DNS サーバ 1 はドメイン `in.it.okayama-u.ac.jp` のセカンダリ DNS サーバとならないように設定され，またドメイン a〜c の TTL（Time To Live）はすべて 0 に設定し，キャッシュが無効になるようにした．図 10 において矢印は DNS 問合せメッセージの流れを示す．

実験結果を**表 1** に示す．この表においてドメイン a〜c の平均値を比較すると，2 種類のレコードのどちらについてもドメイン a，c の値はドメイン b の値のそれぞれ約 3 倍ならびに約 2 倍となっており，DNS プロクシのオーバヘッドはかなり大きいように見える．しかし，図 10 から明らかなように，応答時間の平均値が DNS 問合せ/応答メッセージがネットワーク上を流れる回数にほぼ比例していることから，このオーバーヘッドは DNS プロクシ自身の処理によるものではなく，むしろ DNS 問合せ/応答メッセージの伝送遅延時間によるものと推測できる．また，この程度の伝送遅延時間は通常の DNS の運用においても頻繁に発生するため，実用上問題がないと思われる．

4.4 DNS プロクシの問題点

これまでに，本稿で提案した手法では以下の問題点があることが判明している．

表 1 DNS 問合せに対する応答時間（単位：ms）
Table 1 Response times of DNS queries (in ms).

Type	Dom	Max	Min	Ave	SD
A	a	4.42	2.90	3.14	0.16
	b	2.64	0.97	1.02	0.08
	c	2.95	1.91	2.06	0.11
MX	a	5.64	3.07	3.26	0.15
	b	3.25	1.08	1.17	0.10
	c	5.45	2.03	2.21	0.18

本来の DNS の運用では，複数の FQDN が 1 つのリソースを指し示すとき，そのうち 1 つが正式名（canonical name）となり，残りは別名として CNAME レコードを登録する．しかし，提案方式では，別名ドメインに属する FQDN に対しても CNAME レコードが返されないため，すべての FQDN が正式名として扱われることになる．このため，たとえばある FQDN に対して A レコードを求め，得られた IP アドレスを逆引きして対応する FQDN を求めると元の FQDN と一致しない点が問題となりうる．ただし，正引きと逆引きの両方を行うアプリケーションの多くは，まず IP アドレスを逆引きして FQDN を求め，さらにその FQDN の A レコードを求めて元の IP アドレスと比較するため，両者は一致し，上記のような問題は生じないと思われる．

もし，同一リソースを指し示す既存ドメインと別名ドメインの両方の FQDN が正式名として扱われると問題が生じるような場合，これに対処する方法として，DNS プロクシが CNAME レコードを返す方法が考えられる．しかし，DNS の仕組み上，CNAME レコードと MX レコードの共存が許されないため，この方法では DNS プロクシが MX レコードを書き換えることができず，3.2.2 項で述べた電子メールの配送問題が解決できない．そこで，本研究では電子メールの配送問題がより重要と考え，あえて CNAME レコードを返さない方式を採用した．

DNS プロクシの別の問題点として，virtual host 機能を利用している WWW サーバにアクセスした場合，既存ドメインを用いた URL と別名ドメインを用いた URL では得られる結果が異なる可能性があることがあげられる．すなわち，この virtual host 機能は，同一 WWW サーバに対するアクセスであっても，URL 中に含まれるホスト名が異なればそれを仮想的に異なる WWW サーバに対するアクセスと見なして処理するものであるため，この問題を解決するには DNS プロクシの導入だけでは不十分でありサーバ側での設定変更が必要となる．

しかし，これはむしろ virtual host 機能の特徴とい

うべきものであり，DNS プロクシの問題点とはいえない．すなわち，DNS プロクシは別名ドメインの運用にかかる管理コストを省力化することを主たる目的としているため，どのような手段を用いて別名ドメインを管理・運用してもサーバ側での設定変更が必要になるサービスについては，適用対象外と考えるべきである．なお，電子メールも別名ドメインの導入にともなってサーバ側での設定変更が必要となるサービスであるが，他のサービスとは異なり，基本的にこのサービスだけが参照する MX レコードの存在により，前章で述べたような処理が可能となっている．

5. 関連研究

本手法と同様に DNS プロクシを導入したシステムとして，pdnsd [10]，mDNKit [11] などがある．

このうち，pdnsd は DNS サーバにアクセスできなくなった場合に対処できるように永続的なキャッシュ機能を提供することを主目的としている．しかし，pdnsd には DNS メッセージの書換え機能はなく，複数ドメインの管理省力化に適用できない．

一方，mDNKit は多国語ドメイン名を扱うためのツールキットであり，この中に含まれる mdnsproxy では非 ASCII 文字で表現された国際化ドメイン名を ASCII 文字での表現に変換（正規化）して中継する機能を有している．しかし，mdnsproxy は決められたエンコーディング方式に基づいて 1 対 1 で変換する機能しか有しておらず，たとえ既存ドメイン名に変換できたとしても Authority レコードや Additional レコードの内容を書き換えないため，3 章で述べたような問題が生じることになる．

以上のように，既存の DNS プロクシはいずれも機能的に不十分であり，複数ドメインの管理省力化に応用することは困難である．

6. まとめ

本稿では既存ドメイン名を取得している組織が汎用 JP ドメイン名などの新規ドメイン名を取得した場合，組織内の DNS サーバやメールサーバの設定を変更することなく，既存ドメインと同一の構造を新規ドメインでも利用するための DNS 管理・運用手法として DNS プロクシを提案し，その動作を示した．また，試作した DNS プロクシを試験運用し，実用上有効であることも示した．これにより，特に多くの子孫ドメインを有する規模の大きな組織において複数ドメインの管理・運用のコストを軽減する効果が期待できる．

今後の課題としては，DNS プロクシの機能を拡張し，たとえば特定のホスト名を別名ドメイン用に追加する，別名ドメイン空間に独自のドメインを設定する，特定のサブドメインについて別名ドメイン空間から隠蔽するなど，柔軟な別名ドメインの運用を可能にすることがあげられる．また，今後日本語ドメインでは子孫ドメインについても日本語名を用いたい場合が予想されるので，子孫ドメインまで含めた変換を扱えるように機能を拡張していきたい．

参考文献

1) The Internet Corporation for Assigned Names and Numbers: *New TLD Program* (2001). http://www.icann.org/tlds/
2) 日本ネットワークインフォメーションセンター：汎用 JP ドメイン名 (2001). http://www.nic.ad.jp/dotjp/index.html
3) 松原義継，只木進一：Web ブラウザを用いた DNS 管理システムの開発，情報処理学会分散システム/インターネット運用技術研究会研究報告，Vol.2001-DSM-21-6, pp.31–36 (2001).
4) Internet Software Consortium: *Internet Software Consortium — BIND* (2000). http://www.isc.org/products/BIND/
5) 日本ネットワークインフォメーションセンター：IETF における国際化ドメイン名最新動向，*JPNIC News & Views*, Vol.7 (2001). http://www.nic.ad.jp/jp/pr/MailMagazine/backnumber/vol007.txt
6) Mockapetris, P.: Domain Names — Implimentation and Specification, RFC1035, IETF (1987).
7) Sendmail, Inc.: Sendmail Home Page. http://www.sendmail.org/
8) Nakamura, M.: Information about the Sendmail (2001). http://www.kyoto.wide.ad.jp/mta/sendmail.html#CF
9) Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P. and Berners-Lee, T.: Hypertext Transfer Protocol — HTTP/1.1, RFC2616, IETF (1999).
10) Moestl, T.: The pdnsd homepage (2002). http://home.t-online.de/home/Moestl/
11) 日本ネットワークインフォメーションセンター：多言語ドメイン名に関する技術解説 (2002). http://www.nic.ad.jp/jp/research/idn/index.html

(平成 14 年 4 月 1 日受付)
(平成 14 年 9 月 5 日採録)

山井 成良（正会員）

昭和 59 年大阪大学工学部電子工学科卒業．昭和 61 年同大学大学院博士前期課程修了．昭和 63 年同大学院基礎工学研究科（物理系専攻情報工学分野）博士後期課程退学．同年奈良工業高等専門学校情報工学科助手．同講師，大阪大学情報処理教育センター助手，同大学大型計算機センター講師を経て，現在岡山大学総合情報処理センター助教授．分散システム，マルチメディアシステム，マルチメディアネットワークの研究に従事．IEEE，電子情報通信学会各会員．博士（工学）．

久保 武志

平成 13 年岡山大学工学部情報工学科卒業．現在同大学大学院自然科学研究科博士前期課程在学中．主に広域ネットワークにおける分散システムの研究に従事．マルチメディアシステム，高速ネットワーク等に興味を持つ．

岡山 聖彦（正会員）

平成 2 年大阪大学基礎工学部情報工学科卒業．平成 4 年同大学大学院基礎工学研究科博士前期課程修了．同年同大学院基礎工学研究科博士後期課程を退学し，同大学工学部助手．平成 6 年奈良先端科学技術大学院大学情報科学研究科助手．平成 10 年岡山大学工学部助手．インターネットアーキテクチャ，ネットワーク管理，ネットワークセキュリティの研究に従事．電子情報通信学会会員．

山外 芳伸（正会員）

平成 7 年岡山大学工学部情報工学科卒業．平成 9 年同大学大学院工学研究科博士前期課程修了．平成 13 年同大学院自然科学研究科博士後期課程修了．現在，株式会社ジークス勤務．インターネット運用技術に興味を持つ．博士（工学）．

宮下 卓也

平成 3 年岡山大学工学部電気電子工学科卒業．平成 5 年同大学大学院工学研究科（電気電子工学専攻）修了．平成 8 年同大学院自然科学研究科（知能開発科学専攻）修了．平成 9 年東京農工大学ベンチャービジネスラボラトリー博士研究員．平成 10 年岡山大学総合情報処理センター助手．主にディジタル機器からの放射電磁雑音の計算機シミュレーションの研究に従事．情報処理教育，マルチメディア，高速ネットワーク等に興味を持つ．博士（工学）．IEEE，電子情報通信学会，エレクトロニクス実装学会各会員．