D11-2

学内組織向け DNS ホスティングサービスの運用

前田 光教, 丸山 一貴

東京大学 情報基盤センター

maeda@ecc.u-tokyo.ac.jp kazutaka@ecc.u-tokyo.ac.jp

概要：東京大学情報基盤センターでは、2006 年から学内組織を対象に Infoblox を利用した実験サービスとして DNS ホスティングサービスを開始し、2011 年から正式サービス移行に併せてシステムの更新を行った。本稿では、アプライアンスの Infoblox と仮想マシンの Linux サーバを組み合わせたシステムの構成や、正式サービス移行に伴う運用と課題について報告する。

1 背景

東京大学情報基盤センター（以下、センターとする。）では、教育用計算機システム（ECCS）の他に、学内組織を対象に 2000 年からウェブホスティングサービス[1]、2001 年からメールホスティングサービス[2]、2006 年から実験的に DNS（Domain Name Service）ホスティングサービスを提供している。

東京大学では、u-tokyo.ac.jp ドメイン直下に組織ごとのサブドメインがあり、ほとんどのドメインで学科ごと、研究室ごとにサブドメインが存在している。u-tokyo.ac.jp ドメイン直下であるかどうかにかかわらず、各組織で独自に DNS、メール、ウェブサーバを管理している。サーバの管理はセキュリティの確保、パッチの適用など、ある程度以上の知識を有する必要があるにもかかわらず、管理者の異動や卒業により、あるいは管理者不足により、サーバを独自に管理できないなどのため、センターのホスティングサービスを利用する組織が増え続けている。

DNS ホスティングサービスでは、各組織で管理しているゾーンを、アプライアンスサーバ「Infoblox-1050」（以下、Infoblox とする。）で集中管理するものである。Infoblox は DNS サーバ、DHCP サーバの機能（本サービスでは利用していない）を有し、これらの設定をウェブインターフェイス（以下、GUI とする。）で行うことができる。また、DNS ではゾーンごとに管理権限を委譲する仕組みを有しており、各管理者（センターではドメイン管理者と呼ぶ。）が委譲されたゾーンのレコードやサブドメインの登録、更新を行うことができる。センターでは Infoblox の DNS サーバ、GUI、管理権限委譲の機能を利用しサービスを提供している。

2011 年度からは実験サービスから正式サービスに移行し利用負担金を徴収すると同時にシステムを更新した。

2 システム構成

Infoblox とスイッチの他にセカンダリサーバが 2 台のシンプルな構成（図 1）となっている。

- Infoblox-1050 2 台 （NIOS 5.1）
- Summit X350 1 台 （L2 スイッチ）
- UPS 2 台
- BIND9.7.0 （実マシン CentOS 5.7）
  - SunFire X2200
- BIND9.7.0 （仮想マシン CentOS 5.7）
  - IBM BladeCenter、VMware vSphere

Infoblox は 2 台で Active-Standby の冗長構成とし、Active 側に障害が発生すれば自動的に切り替わる。また、GUI は Active 側に接続することになるが、Infoblox の設定変更やレコードなどの更新があれば、自動的に Standby 側にも同期する。セカンダリサーバの BIND は、Infoblox に登録するすべてをゾーン転送で受けるように設定する。セ

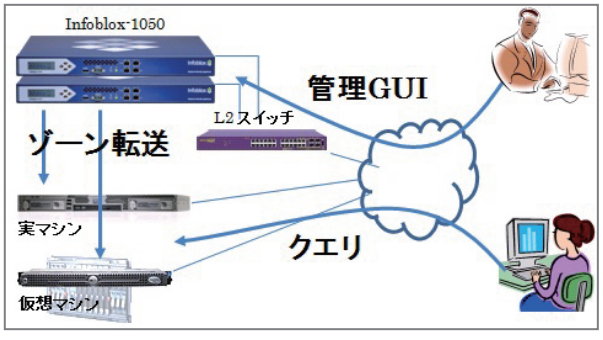


図 1 システム構成図

カンダリサーバの 1 台は実マシンの Linux 上で動作する。もう 1 台はセンターが管理する VMware の仮想サーバ上に Linux の仮想マシンを構築し動作する。

Infoblox は DNS のプライマリサーバにしているが、GUI によるレコードの登録や変更を行うだけとし、エンドユーザからの DNS のクエリを受けるのをセカンダリサーバの 2 台だけとすることで、機能と負荷を分散させた。

セカンダリサーバの 2 台を実マシンと仮想マシンに分けたのは、ハードウェアおよびソフトウェア障害を分散し稼働率を上げるだけでなく、復旧時間の短縮を考慮している。エンドユーザにはセカンダリサーバの 2 台をレゾルバに登録するように要請しているので、実マシンと仮想マシンのいずれか 1 台が生きていれば実害はない。たとえ、Infoblox の 2 台ともメンテナンスや障害で停止しても、ドメイン管理者がレコード等の更新ができなくなるものの、エンドユーザには DNS サービスを継続することができる。

3 運用

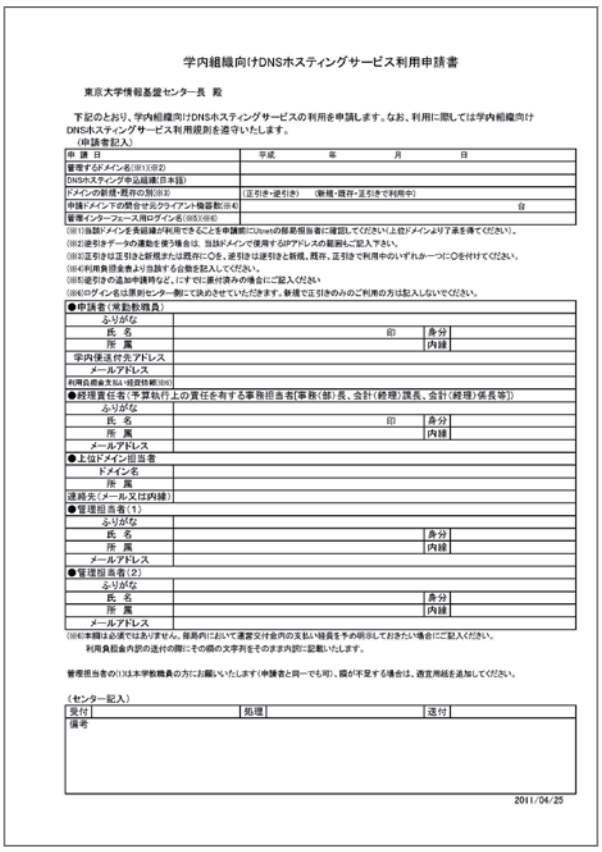
3.1 利用開始までの流れ

○申請者作業、●センター作業

1. ○（新規）上位ドメインにドメインの利用申請
2. ○センターに利用申請書（図 2）の提出
3. ●申請されたドメインが上位ドメインの許可を得られているか確認
4. ●ドメインのゾーンと管理ユーザを登録
5. ●管理ユーザとパスワードの連絡
6. ○レコード、サブドメインの登録
7. ○センターと移行日の日程調整
8. ○エンドユーザへの周知
9. ○●DNS の切り替え作業

センターは、申請書を受理すると、申請されたドメインが申請者の管理するドメインであるかを確認する必要がある。そのため、利用申請書には上位ドメインの管理者に連絡済みかどうかの注意書きを設けた。

センターは申請されたドメインのゾーンと権限委譲した管理ユーザを Infoblox に登録する。セカンダリサーバには Infoblox からゾーン転送を受ける設定をする。登録した管理ユーザとパスワードをドメイン管理者に連絡する。ドメイン管理者は管理ユーザで GUI（図 3）にログインし、レコードやサブドメインの登録を行う。



学内組織向けDNSホスティングサービス利用申請書

東京大学情報基盤センター長 殿

下記のとおり、学内組織向けDNSホスティングサービスの利用を申請します。なお、利用に際しては学内組織向けDNSホスティングサービス利用規則を遵守いたします。

（申請書記入）

申請日	平成　年　月　日
管理するドメイン名(※1)(※2)	
DNSホスティング申込組織(日本語)	
ドメインの新規・既存の別(※2)	(正引き・逆引き)　(新規・既存・正引きで利用中)
申請ドメイン下の問合せ元クライアント機器数(※4)	台
管理インターフェース用ログイン名(※5)(※6)	

(※1)当該ドメインを貴組織が利用できることを申請前にJPnetの部局担当者に確認してください(上位ドメインより了承を得てください)。
(※2)逆引きデータの運用を使う場合は、当該ドメインで使用するIPアドレスの範囲もご記入下さい。
(※3)正引きは正引きと新規または既存に○を、逆引きは逆引きと新規、既存、正引きで利用中のいずれか一つに○を付けてください。
(※4)利用負担金表より当該する台数を記入してください。
(※5)逆引きの追加申請時など、にすでに振付済みの場合にご記入ください
(※6)ログインを(東京センター側)で決めさせていただきます。新規で正引きのみのご利用の方は記入しないでください。

●申請者(常勤教職員)			
ふりがな			
氏　名	印	身分	
所　属		内線	
学内便送付先アドレス			
メールアドレス			
利用負担金支払い経費情報(※6)			
●経理責任者(予算執行上の責任を有する事務担当者(事務(部)長、会計(経理)課長、会計(経理)係長等))			
ふりがな			
氏　名	印	身分	
所　属		内線	
メールアドレス			
●上位ドメイン担当者			
ドメイン名			
所　属			
連絡先(メールまたは内線)			
●管理担当者(1)			
ふりがな			
氏　名		身分	
所　属		内線	
メールアドレス			
●管理担当者(2)			
ふりがな			
氏　名		身分	
所　属		内線	
メールアドレス			

(※6)本欄は必須ではありません。部局内において運営交付金内の支払い経費を予め明示しておきたい場合にご記入ください。
利用負担金内訳の詳細にその欄の文字列をそのまま内訳に記載いたします。

管理担当者の(1)は本学教職員の方にお願いいたします(申請者と同一でも可)。欄が不足する場合は、適宜用紙を追加してください。

（センター記入）

受付	処理		送付
備考			

2011/04/25

図 2　DNS ホスティング利用申請書

既存の DNS サーバを管理していた組織では DNS ホスティングサービスへの移行が必要である。現在までの移行は、既存の DNS サーバを運用しながら DNS ホスティングサービスにも同じレコードを登録し、ある日時に切り替えた。ドメイン管理者は、同時に上位ドメインの管理者へ DNS サーバの IP アドレス変更を連絡する。

切り替え日時は、ドメイン管理者がセンターと調整するとともに、エンドユーザの各クライアン

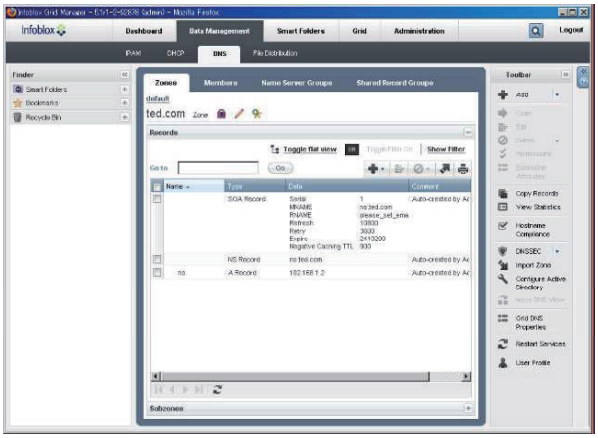


図 3　管理インターフェイス

トのレゾルバの変更が必要になることを十分に周知するよう配慮して決定する必要がある。

既存の DNS サーバからの移行では、BIND の設定とレコードを変換するツール「Data Import Wizard」が Infoblox 社で提供しており（図 4）、そのツールによって作成されたファイルを Infoblox にアップロードすることで、移行がほぼ完了する。

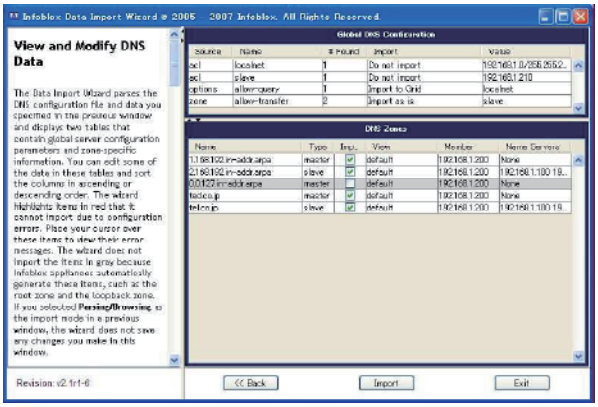


図 4　Data Import Wizard

3.2　継続処理

センターでは、サービス利用組織に対して、年度ごとに継続処理を行っている。昨年度までは実験サービスの無料であったため、メールによる継続意思の確認だけであった。本年度からは利用負担金が発生することから、書面による継続申請書を提出してもらう予定である。継続申請書の提出は本年度末からの作業となるが、センターのウェブやメールホスティングサービスでも同様の作業を行なっており、それに倣って行う予定である。実際には、ドメイン管理者に継続申請書を送り、申請情報（管理者名等）の変更には赤字で訂正し、申請者と経理担当者は押印して返送することとなる。

正式サービス移行に当たっては、無料から有料になることを説明し、同意していただくことで継続の意思を確認した。

3.3　利用負担金

利用負担金は、申請時に申告されたクライアント機器の台数またはゾーンの登録レコード数の大きい方をもって料金（表１）を決定することとした。

表１　利用負担金

台数またはレコード数の大きい方	年額利用負担金
1～ 20	10,000 円
21～ 50	20,000 円
51～ 100	30,000 円
101～ 200	50,000 円
201～ 500	70,000 円
501～1000	100,000 円
以降＋1000	30,000 円

3.4　ユーザ対応

ドメイン内のエンドユーザはドメイン管理者に、ドメイン管理者はセンターに問い合わせすることとした。センターはドメイン管理者からのものに限定することで、問い合わせ対応の負担を軽減している。このような対応方法は、既に正式サービスとして運用しているウェブやメールホスティングサービスに倣っており、周知が進んでいることもあり、各ドメイン管理者には理解していただいている。

4 課題

4.1 利用申請

センターに利用申請書が届いても、申請するドメインが申請者の管理するものなのかどうかについてセンターは把握していない。また、その上位ドメインの管理者を把握していない。そのため、利用申請書には項番 3.1 に示したような注意書きを設けた。実験サービス中は、申請があると関係する組織（一部はセンター内のネットワーク担当係）に連絡し、

- 正しく申請されたドメインか
- ドメインの管理者は誰か

などの確認作業を行っていた。DNS はその仕組み上、管理するドメインの上位が存在し、管理するドメインを受け持つサーバの情報を上位ドメインのサーバに登録する必要があるが、申請者が所属組織のドメイン申請の手順を確認しないまま利用申請するケースがあった。センターは申請された上位ドメインの管理者を特定し、申請者には DNS

サーバの利用目的を問い合わせるなど、各所の調整に多くの時間を割くこととなった。最終的には申請されたドメインは独自の DNS サーバを必要としない方法で目的を達成できることがわかったため、申請は取り下げられた。

正式サービス移行後間もない現在は、ドメイン管理者の DNS のリテラシーが高いこともあり、GUI の質問がある程度で DNS の仕組みから説明することは稀であるが、先のようなケースが増えることを考慮する必要がある。u-tokyo.ac.jp ドメインの一部はセンター内のネットワーク担当係が管理しており、連絡を密に行うことが課題と認識している。また、利用者向けには本サービスを利用するための登録手順を広報する必要がある。

4.2 利用負担金

正式サービス移行で負担金の料金を決める根拠で議論が大いになされた。商用サービスと違い、ドメイン名と IP アドレスの変換だけを行うサービスと、エンドユーザがレゾルバとして直接クエリ受けるサービスが含まれているため、料金はサーバの利用量で決めるのが最も平等であり、それはサーバへのクエリ数と考える。しかしながら、ある日を境にしてログ等から組織ごとのクエリ数をカウントしなければならず、センターの負担が増えるだけでなく、ドメイン管理者が負担金の予想が立たないことから受け入れてもらえないと判断した。ゾーンの登録レコード数だけではサーバの利用量と比例する根拠とならないため、DNS ホスティングのサーバへ直接クエリを送るクライアント数を申告してもらい、レコード数とクライアント数で多い方を負担金の元とすることにした。その数には、ルータなどで DNS 情報をキャッシュしてクライアントからのクエリをそのルータで処理する場合は、そのルータの数だけを申告すれば良いこととした。しかしながら、負担金の根拠については今後も検討すべき課題と認識している。

5 まとめ

Infoblox はアプライアンスサーバであり、ゾーンやレコード等の登録、更新のための GUI を持つため、センターのサーバ管理の容易さだけでなく、ドメイン管理者は、GUI の慣れは必要であるものの、BIND の設定の知識がなくても DNS の管理が容易に行える。センターは、ゾーンの管理権限を委譲できるため、運用コストを大幅に軽減できている。

2011 年 10 月現在の登録数は 18 組織（表 2）と決して多いものではない。各組織で運用されている DNS サーバは頻繁に更新するものではなく、一旦運用に入ると機器の更新や故障といった契機がないと見直されない傾向がある。ウェブやメールホスティングサービスの登録数推移を考察すると十分な需要はあると考えられ、今後、登録数は緩やかに増加すると見込まれる。また、正式サービス移行後の登録は 1 組織であり、サービス移行による影響を考察するほどの段階ではないので、今後、報告していきたい。

表 2 登録組織（一部抜粋）

組織単位	レコード数	クライアント数
学部・研究科	94	1,300
学部・研究科	219	1,000
附置研究所	1,765	2,000
学部・研究室	12	10
全学センター	300	255

参考文献

[1] 坂井 朱美、丸山 一貴、関谷 貴之、有賀 浩、岩藤 健弘、「学内向け Web ホスティングサービスの運用」、平成 22 年度 情報教育研究集会講演論文集、149-152 ページ、2010

[2] 秋田英範、丸山一貴、関谷貴之、佐々木馨、増田均、「学内向けメールサービスの運用と稼働状況について」、平成 21 年度 情報教育研究集会 講演論文集、437-440 ページ、2009