

Title	Proxyシステム
Author(s)	上埜, 元嗣
Citation	国立大学法人北陸先端科学技術大学院大学技術サービス部業務報告集 : 平成23年度: 23-26
Issue Date	2012-08
Type	Others
Text version	publisher
URL	http://hdl.handle.net/10119/10799
Rights	
Description	

Proxy システム

上埜 元嗣

情報社会基盤研究センター

概要

情報社会基盤研究センターでは全学サービスとして WEB の proxy サービスを提供している。高速な外部へのアクセスや安全な通信を目的としているが、最近ではインターネットの高速化もあり高速な外部へのアクセスにはあまり貢献できていないという側面もある。本稿では一昨年のシステム更新から現在までの運用およびそれに伴う問題点や課題について報告する。

1 はじめに

Proxy サービスは情報環境の一部であり 4 年に 1 度機器の更新が行われている。更新時にはシステム構成の見直しにはちょうど良い時期である。2010 年での更新では 3 台（一部他サーバとの共用）のサーバで構成していたが、2 台のサーバに統合した。また、更新後は最近通信量が多くなっているストリーミングやソフトウェアのアップデートなどで、通信障害などが出たりなどもあったが、現在は問題なく運用できている。本稿ではシステム更新の際のサーバの統合、更新後に起きた問題について報告する。

2 システムの更新

2009 年度の情報環境調達に proxy システムの更新が盛り込まれている。実際機器が設置されたのは 2010 年の 2 月頃であったが、設定やテストなど行い旧システムと入れ替えたのは 7 月であった。旧システム proxy 自動設定用サーバ（web サーバと兼用）、proxy サーバ、AntiVirus サーバの 3 台のサーバから構成されていたが、新システムでは、proxy 自動設定を proxy サーバで配布できないかを検討した。Proxy サーバは旧システム新システムともに専用装置を使用しているが、旧システムは NetApp 社 NR1000C230 を、また、新システムは BluCoatSystems 社 SG810/AV810 シリーズを採用した。

2.1 BlueCoat SG810-10/AV810-B

BlueCoatSystems 社 SG810-10（以下 SG810）と AV810-B（以下 AV810）を新しい proxy システムとして導入した。SG810 は proxy サーバであり、AV810 は AntiVirus サーバである。これらを統合して使用することにより高速で安全な proxy システムを構成する。主な特徴としては

- スケーラビリティとパフォーマンス
SG810 と AV810 を合わせて構成することにより Web オブジェクトをワイヤースピードで分析（最大

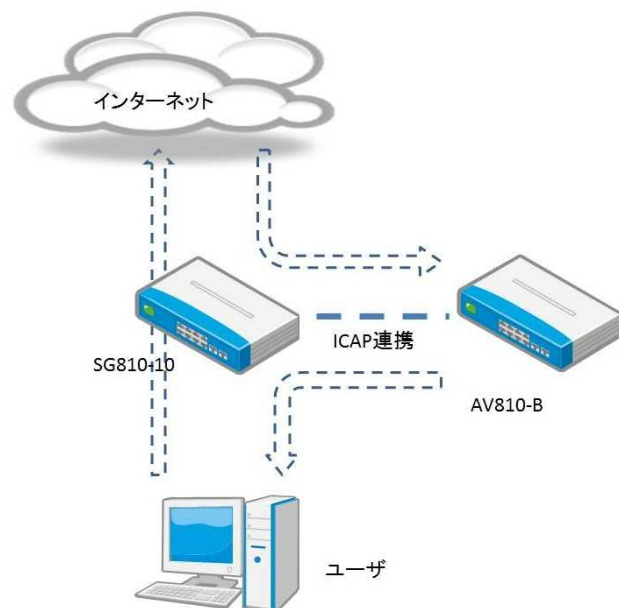


図1. システム構成図

240Mbps,7-9 ミリ秒の遅延

- 階層型のセキュリティと防御

3 Proxy 自動設定の配布

Proxy 自動設定 (Proxy Auto Configuration 以下 PAC) はクライアントの Web ブラウザの Proxy 設定を自動で行うためのものである。この方法は何通りかあるがなるべく

多くのユーザに proxy サーバを使用してもらうためにはユーザが設定しなくても配布できるほうがよい。



図2. BlueCoatSG810-10

3.1 WPAD

WPAD とは Web Proxy Auto-Discovery Protocol の略であり、Web ブラウザなどの設定を自動化するために開発されたプロトコルである。DHCP・DNS・HTTP を組み合わせて設定され、これによりユーザおよび管理者の負担が軽減される。WPAD は Internet Explorer、Mozilla Firefox、Safari などの有力なブラウザでサポートされており、学内ユーザのほとんどがこれらの web ブラウザを使用している。情報社会基盤研究センターでは主に Mozilla Firefox を推奨している。本学では 2005 年よりこの方法を運用している。本学の場合下記の URL に自動的にアクセスし PAC を読み込み Proxy の設定が自動的に設定される。

`http://wpad.jaist.ac.jp/wpad.dat`

このサーバは PAC を記述したファイルを http でアクセスできる URL で公開すればよい。それまでは既存の Web サーバで上記 URL にて PAC が公開されるように設定していた。

3.2 SG810 での WPAD の設定

ホスト名は DNS で SG810 の IP アドレスに対し `wpad.jaist.ac.jp` を割り当てる。

SG810 の設定を行っているうちに PAC の設定が可能で、PAC ファイルをそのままアップロードできることが分かった。しかしながら、PAC の公開 URL がシステムで下記 URL で固定になっていて変更できないこともわかった。

`http://server:8081/accelerated_pac_base.pac` (ただし server は IP アドレスを設定すると変更される)

そこで、Policy Rules に URL の rewrite を追加し `http://wpad.jaist.ac.jp/wpad.dat` に対し要求があった場合上記の URL に書き換えを行う設定を追記した。

WPAD で用いられる URL 以外にもいくつか PAC 公開していた URL が存在していたので、複数の URL を書き換える可能性を考慮し下記のルールを定義した。

```
define action rewrite_wpad
  rewrite( url, "(.*)", "http://150.65.7.77:8081/accelerated_pac_base.pac" )
end
```

次にこの定義を利用し書き換えたい URL を定義した。

<Proxy>

```
url=http://wpad.jaist.ac.jp/wpad.dat action.rewrite_wpad(yes)
```

これにより WPAD をの要求を SG810 単体で処理できた。これまで兼用の Web サーバのメンテナンス時などにも URL を公開するため別の Web サーバに設定を移動したりしていたがその部分では管理コストが減ることになった。

4 運用中における問題

SG10 の設定がある程度完了し、全学に向け旧システムから入れ替え新システム SG810/AV810 での運用を本格的に始めた。運用としては、定期作業、問題対応などがあげられる。問題点及びその対応をいくつかあげる。

4.1 ファームアップ時の問題

ファームウェアのアップデートを行う際は SG810・AV810 とともに再起動する。再起動の間 2~3 分程度かかるわけだが、proxy サービスを利用しているユーザに不便をかけることとなる。なるべく再起動の回数を減らすためにネットワークのメンテナンスや計画停電時などに合わせて作業を行っているが、アップデートが公開されてから時間がたってしまう。図 1 にあるように AV810 はユーザ端末とは直接通信をしないことから、AV810 だけでもユーザの通信を妨げることなくアップデートできないか検討した。SG810 の ICAP 連携の設定と policy 設定を変更し AV810 が通信できないときは AV810 でデータスキャンせずにユーザ通信を返すことで回避できることとした。セキュリティ観点からは本学セキュリティポリシーにてユーザ端末は端末自身でセキュリティの配慮をもちいることが明記されているので問題ない。

4.2 ダウンロードできないストリーミングデータ

ストリーミングについても proxy を経由している。ストリーミングデータはいくつもの種類があり同じ形式でも通信プロトコルも違っていたりする。audio/aac という MIMEType を使ったストリーミングが AV810 を経由するとダウンロードできないという問題がおきた。当然 proxy を経由しなければ問題がない。そこで、SG810 の policy を使い以下の 3 点を検証した。

- キャッシュのみ行わない
- AntiVirus チェックのみ行わない (AV810 を通さない)
- キャッシュおよび AntiVirus チェックを行わない

結果 AntiVirus チェックを通さなければダウンロードできることが確認でき、audio/aac に関しては SG810 の policy で AV810 での AntiVirus の check をしないように設定することで解決した。

4.3 その他

Adobe Reader や Adobe Flash を初期インストールする場合に proxy 経由だとインストールできないという問題が最近報告された。Adobe 社でもこの問題は認識しており調査中という報告がある。我々も検証し policy などを設定することで解消できるかどうか、今後検証し対応していきたい。

5 統計

以下に現在の一部の統計データを挙げる。

5.1 ユーザ数

図3は一日のユーザ数を時系列でグラフに表わしたものである。授業などの開始時間から徐々に増え16時をピークに減っている。しかしながら、深夜でも一定のユーザがいることがわかる。

図4は一ヶ月間のユーザ数を時系列で表わしたものである。週末は半分程度に減ってはいるもののやはり一定数のユーザがいることがわかる。24時間毎日の安定運用が必然であると再認識した。

5.2 キャッシュされたコンテンツ

図5にはキャッシュデータをサイズ別に数に表わしたものである。グラフは縦軸が対数目盛で表わしたものである。1KBから50KBまでのサイズが多く存在している。Webページなどの小さいコンテンツがよくキャッシュされていることがわかる。

6 まとめ

システムの更新作業や問題への対応を行っている中でSG810とAV810を合わせた構成では複雑な設定ができいろいろな状況や要望にも対応できることが分かった。また、統計からユーザも日時で差があるが常時一定以上のユーザが利用していることもわかった。今ある問題点はこれから検証し対応するが、これからも重要なシステムの一つとして安定運用を保っていきたい。

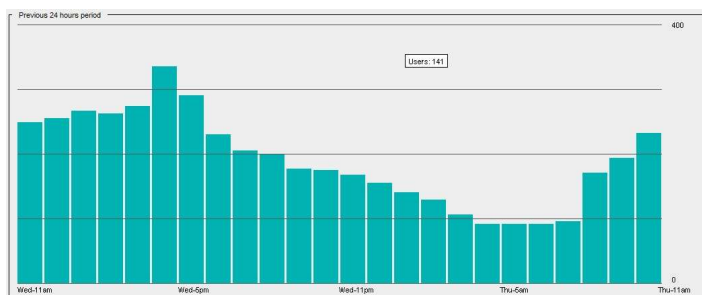


図3. 1日(AM11:00から)の利用者の推移

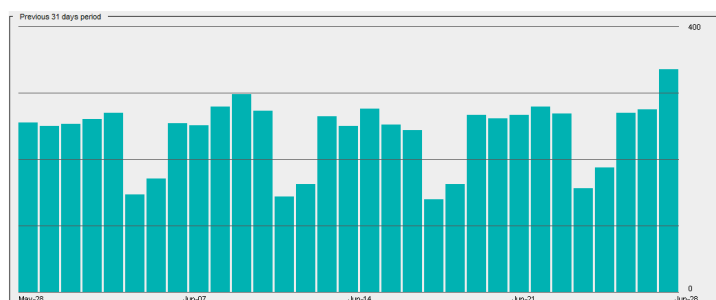


図4. 一ヶ月間の利用者推移

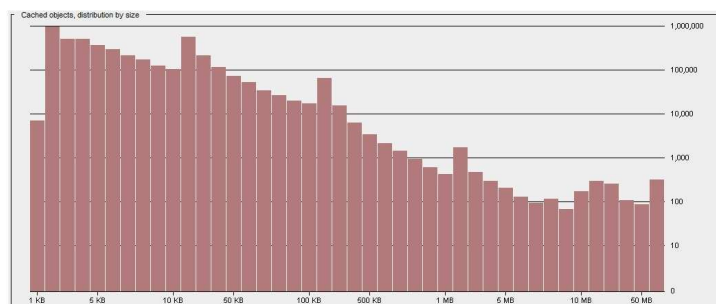


図5. キャッシュされたコンテンツのサイズ別数