



注意したい7つの落とし穴  
Blue Coat SGシリーズ構築における  
Sierのための実践講座

本講座は、ITエンジニアの為の明日から役に立つシステム構築スキルや技術・製品スキルなどをご提供します。まだお客様へご提案したことがない製品や技術でも、ポイントを押さえた実務知識を短時間に把握したい方にお勧めです。

【今回の講座】

今回は、高速化とセキュリティ機能を併せ持つセキュア・プロキシ・アプライアンス製品であるBlue Coat SGの機能について紹介しながら、本製品の導入時や運用時に見ておきたいポイントをわかりやすく解説します。

By 芦田 勲  
Macnica Networks Corp.

社内ユーザのWebアクセスを管理するためにも必要不可欠な存在になっているプロキシサーバ。これまでユーザが求めるプロキシサーバの役割は、キャッシュ機能によるWebの高速化が主でしたが、最近では社内ネットワークのWebセキュリティ対策を強化するための高度な機能を求めて導入を進める企業が主流となっています。

1. セキュリティ強化は“代理”に任せろ！プロキシの役割と製品の特長
2. 7つのポイントが明暗を分ける！Blue Coat SG構築術

## 1. セキュリティ強化は“代理”に任せろ！プロキシの役割と製品の特長

### プロキシとは“代理”のこと

単純にプロキシを直訳すると「代理」という意味になります。これは、クライアントの代理としてWebサーバにアクセスを行うという役割からきているためです。このプロキシサーバがクライアントのWebアクセスを仲介することで、不正なアクセスを制御するなどセキュリティが強化され、一度表示したページをプロキシサーバ側でキャッシュとして溜め込むことによってトラフィックを軽減することが可能になります。このプロキシサーバの設置形態は、大きく2種類に分けることができます。社内LANから外部（インターネット等）へのアクセスを中継するフォワードプロキシ構成と、特定のサーバの代理として外部からサーバへのアクセスを中継するリバースプロキシ構成です。

### Blue Coat SGシリーズが持つ4つの特長

Blue Coat SGは、Webアクセスを高速化するためのキャッシュ機能に加え、多様なセキュリティ機能を有しています。代表的なものには、ユーザ認証、コンテンツフィルタ、Webウイルス/スパイウェアの検知・除去、HTTPSの通信の制御・可視化などのセキュリティ機能があります。それぞれの特徴は以下のとおりです。

#### ●ポリシーを適用するユーザ認証

LDAP、ActiveDirectoryなどの認証サーバと連携することで、ユーザやグループ単位でポリシー設定が可能になります。認証ユーザIDはアクセスログにも反映され、DHCP環境でもユーザの利用状況を把握することができるようになります。

### ●外部データベースも柔軟活用！コンテンツフィルタ

国内外で提供されている複数のURL/コンテンツフィルタリングベンダのデータベースをBlue Coat SGで利用することができます。データベースは、Blue Coat SGの内部で保持しており、「ポルノ」サイトなど不適切なサイトへのアクセスを禁止することが可能となります。

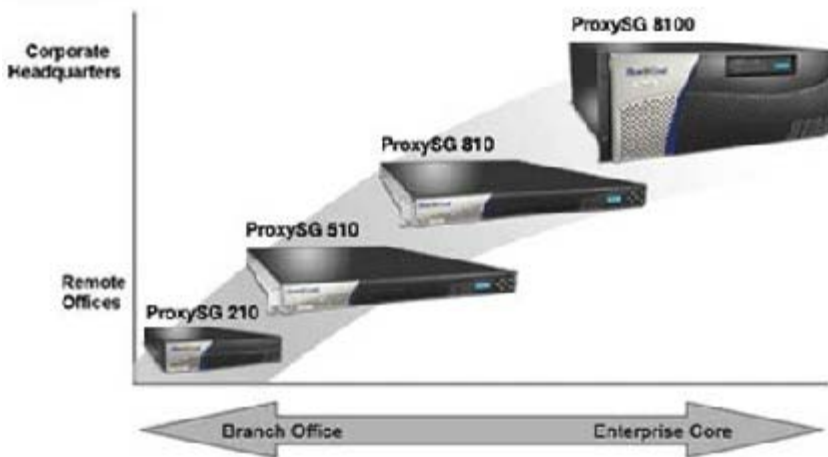
### ●怪しいサイトには近づけない！Webウイルス/スパイウェアの検知・除去

ICAPを利用してウイルススキャンサーバであるBlue Coat AVと連携し、ウイルスに感染しているWebコンテンツを検知・除去することができます。

### ●暗号しただって見逃さない！HTTPS通信の可視化・制御

SSLプロキシ機能を用いることにより、SSLトラフィックをコントロールできる。そのため、暗号化されているHTTPS通信をBlue Coat SGで複合化し、SSLをくぐり抜けようとするスパイウェアやウイルスを防ぐことが可能となります。

次に、Blue Coat SGのハードウェアモデルについて紹介します。小規模から大規模まで4つのモデルがラインナップされており、様々なインターネット環境に対応しています。



### 遅延のない高速化にも寄与！プロキシ以外の機能

Blue Coat SGでは、プロキシ機能以外にもWAN最適化テクノロジーMACH5が搭載されています。オブジェクトキャッシュ、プロトコルの最適化、圧縮、バイトキャッシュ、QoS機能を組み合わせることにより、WANを介してやり取りされるビジ2. 7つのポイントが明暗を分ける！Blue Coat SG構築術  
ネスアプリケーションを高速化し、パフォーマンスを向上させることができるようになります。

## 2. 7つのポイントが明暗を分ける！Blue Coat SG構築術

基本的な機能を見てきたところで、いよいよ構築にあたって押さえておきたいポイントを紹介しましょう。ここでは、Blue Coat SGをフォワードプロキシで利用する場合を例にとり、導入前、導入時、運用という流れで順に解説していきます。

### 導入前のポイント

#### ●ポイント1:「機器のサイジング」は端末台数とスループットで

まず、必ず導入前に必要になるのは、ユーザ環境に安定して動作するモデルを選定することです。Blue Coat SGシリーズのモデルの選定を行う際は、Max Active Desktopsにてサイジングを行います。この“Max Active Desktops”とは、プロキシサーバを利用してWebアクセスを行う可能性のあるクライアント端末の総台数を指します。

例えば、端末が500台規模の場合には、Max Active Desktopsが500以上になるSG510-10相当のモデルを提案することになります。しかし、50Mbps以上のスループットがユーザ要件として求められている場合、Max Active Desktopsそのものはスループットを考慮していないため、別途サイジングが必要になってきます。なお、Blue Coat AVシリーズのサイジングはBlue Coat SGシリーズと対になっており、別途アクセス数などでサイジングする必要はありません。

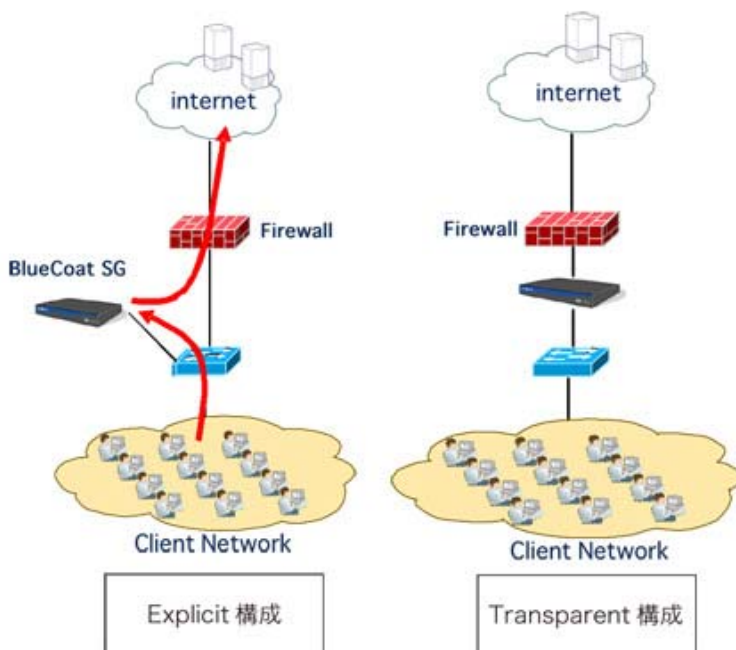
#### ●ポイント2:プロキシ指定か否かで構成が変わる

次に、ユーザ環境におけるクライアント端末のブラウザ設定でプロキシサーバが指定されているか確認する必要があります。プロキシ指定の有無で提案構成が変わってくるからです。

Explicit構成とは、クライアント端末がブラウザの“プロキシサーバの指定”に該当のプロキシを設定し、プロキシサーバ経由でInternetアクセスを行うものです。最もスタンダードな構成になります。

一方、プロキシ指定をしていないクライアント端末からのアクセスをプロキシサーバで制御させたい場合は、Transparent構成を用いることで実現できます。Transparent構成では、クライアント端末がInternetアクセスを行う経路上にBridgeとしてBlue Coat SGを挟み込む必要があります。ちなみに、機器が故障した際にも通信が止まらないようBlue Coat SGにはパススルーカードが装備されており、電源障害時でも通信断が発生しない仕組みになっています。

また、Explicit構成の場合は、FailOver機能(Active-Standby)を用いるか上位のロードバランサで振り分けることで、冗長性を保つことが可能です。



### ●ポイント3: ユーザ環境の把握で気をつけたい“ロギング状況”

当然ながら、ユーザ環境が現在どのように動作しているか把握しておく必要があります。上位にプロキシサーバやVirusScanサーバが存在している場合は、多段プロキシ構成にする必要があるかどうかの判断が必要になり、既存プロキシをリプレースする場合は、どのようなプロキシサーバが入っているかどうかを把握しておかなければいけません。

例えば、上位にプロキシサーバなどが存在している場合は、上位プロキシで送信元IPアドレスのロギングを行っているか確認する必要があります。上位プロキシでは、送信元IPがクライアントIPではなくプロキシサーバのIPアドレスになるので、上位で送信元IPアドレスによる判別ができなくなってしまう。その場合の回避策としては、上位プロキシに転送する際にHTTPヘッダ(X-forwarded-for)にクライアントIPを付加することで、上位プロキシはロギングすることが可能になります。ただし、上記回避策は上位プロキシがX-forwarded-forを理解できることが前提となります。

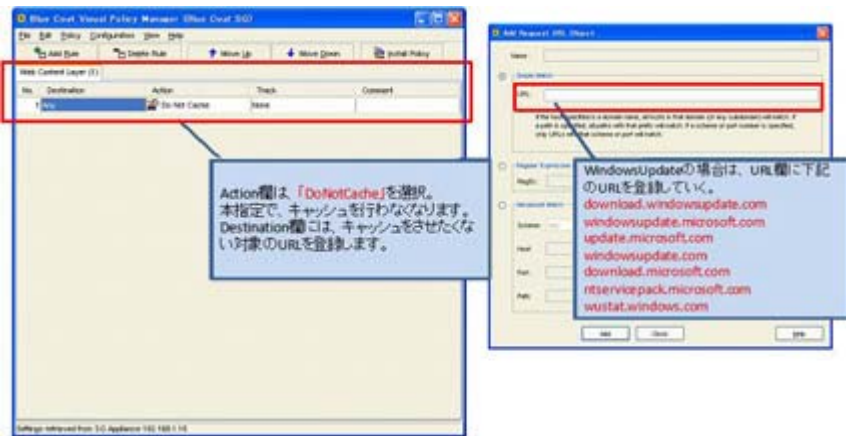
### 導入時のポイント

次に導入時に見ておきたいポイントを紹介しましょう。特にキャッシュ、ウィルススキャン(ICAP連携)に関して注意が必要ですが、考慮すべきポイントは2つ挙げられます。

### ●ポイント4: キャッシュ回避の“Windowsアップデート”を忘れずに

Windowsアップデートのサイトをプロキシサーバでキャッシュしていると正しくアップロードできない場合があります。そのため、Windowsアップデートのサイトは、キャッシュさせないというポリシーを追加して回避する必要があります。また、イントラサーバへのアクセスはInternet回線を使用しないため、キャッシュさせる意味がありません。このような通信ある場合は、キャッシュさせないポリシーで導入するケースが多いです。

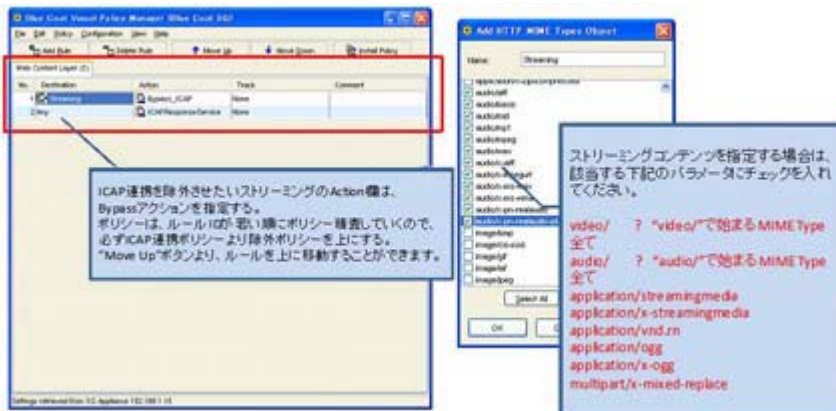
具体的には、VPMよりWeb Contents Layerを作成し、「Destination」のRequest URLのSimple Matchの指定にURLを、「Action」に「DoNotCache」を指定する事でキャッシュを行わないように設定できるようになります。



### ●ポイント5: VirusScanはファイルサイズの大きさに気をつけたい

ストリーミング系、オーディオ系などコンテンツサイズが大きいファイルをVirusScan対象とした場合、Blue Coat AVを含めたVirusScanサーバのリソースを圧迫してしまい、ユーザサイドレスポンスを低下させる場合があります。例えば、MIME Typeに関しては、下記手順によってVirusScan対象から外すことをお勧めします。

VPMのWeb Content Layerより、Destination ObjectとしてHTTP MIME Typeを選択することで対象から外すことが可能です。

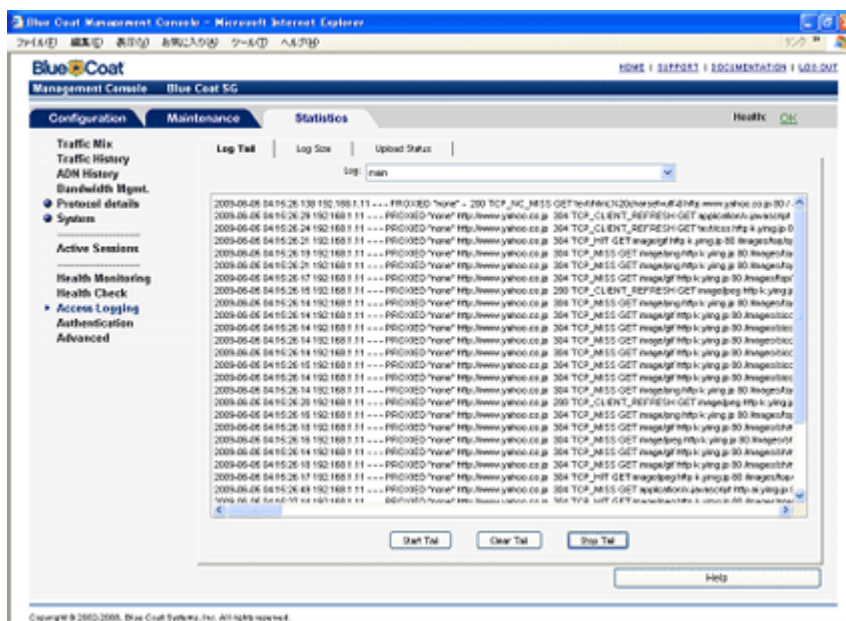


### 運用のポイント

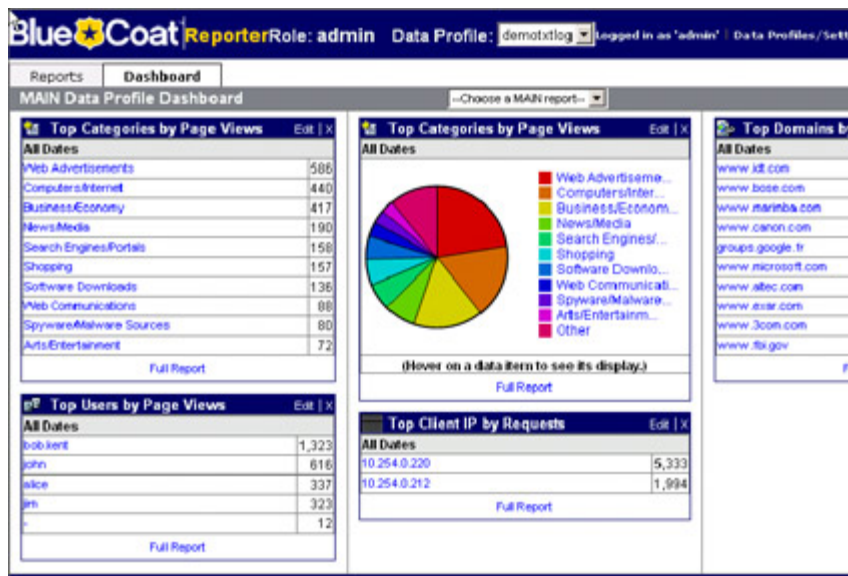
最後に、日々のアクセスログ解析やプロシ設定の変更など運用時に見ておきたいポイントを2つ紹介します。

#### ●ポイント6: かゆいところに手が届くアクセスログ解析ツール「Reporter」

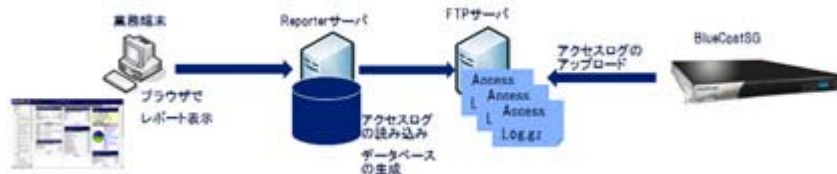
Blue Coat SGでは、直近のアクセス状況であれば、WebUIで閲覧することができます。しかし、古いアクセスログはWebUIで確認することができないため、アクセスログ格納用のFTPサーバを準備しておき、一旦ログをアップロードしてから閲覧する運用になります。しかし、いずれもテキストベースになるため、解析は困難になってしまいます。



そのような状況を改善するため、Blue CoatではReporterという解析ツールをソフトウェアで提供しています。Reporterを用いることによって、インターネットのアクセス状況をビジュアルに表示することができるため、アクセス状況が簡単に調査することが可能です。



アクセスログ解析ツールであるReporterは、別途サーバが必要になります。そのため、Reporterを運用しているユーザの多くが、アクセスログ格納サーバとReporterサーバを兼用して運用しているのが一般的です。ちなみに、ReporterとBlue Coat SGの関係は下記のようにイメージするとわかりやすいです。



ただし、Reporter用のサーバはどのようなものでも問題なく動作するというわけではありません。サポートしているOSと安定して動作するサーバスペックを考慮する必要があります。

現時点 (v8.3.5.2) でサポートしているOSは下記の通りです。

- ・ Windows XP, 2000, and 2003 Server
- ・ Red Hat 9 and Red Hat Enterprise AS/ES 4 and AS/ES 5 (32bit)
- ・ Red Hat Enterprise Linux AS release 4 and AS 5 (64bit)

また、サーバスペックのサイジングは、アクセスログ量とReporterで閲覧したい期間によってスペックが異なるので注意が必要です。

### ●ポイント7: 手間もリスクも回避したいPolicy設定のリストア方法

複数のBlue Coat SGが同じPolicyで稼働している場合、1台のPolicyを変更すると他のBlue Coat SGのPolicy設定も当然変更しなければなりません。ただ、手動で設定変更していくと設定変更の箇所が多いとそれだけ手間と時間がかかってしまい、ミスも増える可能性があります。そこで手間やリスクを軽減する方法としては、Policy Fileでのリストアを行うことにより簡単に変更することができます。

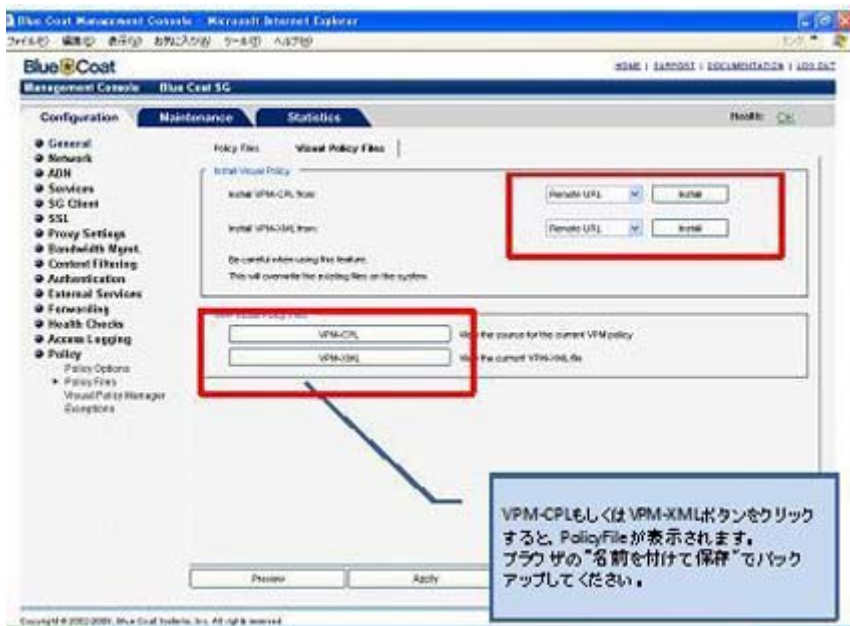
# LANch BOX online Magazine

夏号 2009

1台目については手動での変更が必要ですが、1台目のPolicy Fileのバックアップを取得しておけば、そのファイルを用いて他の機器にPolicyのみをリストアすることが可能となります。手順は、WebUIで、Configuration → Policy → Policy Filesで下記のような画面が表示されるため、VPM-CPLとVPM-XMLの2種類とも取得しておきます。

VPM-CPLとVPM-XMLの役割ですが、VPM-CPLがBlue Coat SG内部で動作しているポリシーのコマンドになり、VPM-XMLがVPMで表示されている画面レイアウトになります。

リストアする際は、Install Visual Policy欄で保存した各ファイルを”Install”ボタンよりリストアすることができます。



さらに導入やコンフィグレーションなど詳細を習得したい方には、国内で唯一ブルーコート社が認定している有償の Authorized Trainingプログラム(アドミニストレータコース/プロフェッショナルコース)もありますので参考にしてください。

芦田 勲

大阪を拠点に西日本エリアで活動しているエンジニア。ロードバランサ、プロキシ、WAN高速装置などアプライアンス製品中心に提案構築を行っている。Blue Coatの構築実績は多数。

<参考>

- ・ Blue Coat SG製品詳細  
[http://www.macnica.net/bluecoat/sg\\_av.html](http://www.macnica.net/bluecoat/sg_av.html)
- ・ Blue Coat Systems認定トレーニング<有償・定期>  
<http://www.macnica.net/bluecoat/training.html>
- ・ Blue Coat 導入実践セミナー<無償・定期>  
[http://www.macnica.net/bluecoat/seminar\\_01.html](http://www.macnica.net/bluecoat/seminar_01.html)