大規模組織のためのトラフィック量追跡管理と使用量割り当て制限

はじめに

自分のデスクから企業内 VPN やインターネットなどのデータ通信ネットワークに接続するのが当たり前になった今、こうした機能のない業務環境など想像するほうが難しいと言えます。ネットワークへのアクセス機能は、事業内容にかかわらず、電話同様に不可欠の道具になっているのです。実際、音声通話機能はデータ通信ネットワークに組み込まれる傾向にあり、デスクから LAN に接続するだけで、電話、アプリケーション用データ、マルチメディアといったサービスが一元的に利用可能になっています。

このように、デスクにいながらにしてデータ通信サービスが利用できる環境は急速に広まっているにもかかわらず、データ通信サービスほどに普及していないのが、アカウンティングや制御の機能です。電話に関しては、通話 1 件 1 件に至るまで追跡管理し、ユーザーごとに通話可能な相手をきめ細かく設定する発信許可機能までありながら、ネットワーク利用となると、誰が何のためにどのくらい使っているのか、正確に把握していない組織が少なくありません。たとえ把握できたとしても、その管理方法と言えば、せいぜいユーザーに対して使用上のポリシーを通知する程度にとどまっています。ほとんどの場合、こうした環境では、ネットワーク側で一元的にポリシーを適用する体制が欠けているのです。

昔のように、ネットワークの利用が一部の信頼のおけるユーザーだけに限定されていて、ネットワークアクセスの予算も通信関連コスト全体のごく一部にとどまっていた時代であれば、ネットワーク側でのポリシー適用がない状態でも何とかなるかもしれません。しかし、すべてとは言わないまでも、もはやこのような状態が成り立たないケースのほうが多いのではないでしょうか。

そこで、このホワイトペーパーでは、ネットワークアカウンティングと利用ポリシー実施のあり方について考察します。なお、関連のテーマとしては、ファイアウォールとセキュリティがありますが、今回のテーマから外れるため取り扱いません。

フローベースのアカウンティングと制御

フローベースのアカウンティングは、ベンダ各社からさまざまな名称でソリューションが提供されています（ジュニパーネットワークスの場合は「J-Flow」）。名称こそ違いますが、フローレコードのフォーマットは共通しています。名前からもわかるように、フローアカウンティングの基本は「フロー」です。このフローとは、送信元と宛先の間でどちらか一方に向かうデータの流れです。各フローには、次の情報が含まれています。

- 送信元 IP アドレス
- 宛先 IP アドレス
- 送信元ポート番号
- 宛先ポート番号
- レイヤ 3 のプロトコルタイプ（TCP、UDP、SCTP、DCCP）
- TOS（Type of Service）
- 入力論理インタフェース

フローデータ収集はアカウンティングに有効であるだけでなく、トラフィックエンジニアリングやネットワーク容量計画のほか、セキュリティモニタリングにも役立ちます。通常、フローアカウンティング機能は、ルーターや一部のインライン型モニタリング装置に組み込まれています。基本的には、トラフィックを監視して、フローごとにフローレコードを作成します。このフローレコードには、上記の基本情報のほか、フロー内のパケット数やバイト数も含まれます。1 つのフローが完了すると、フローに関するレポートが作成されます。複数のフローレコードを結合して、1 つのフローパケットにまとめることも可能です。このフローパケットは一種の IP パケットのため、別の場所にあるフローデータ収集システムに送ることができます。収集システムがどこに置かれていても、直接接続されている収集システムのインタフェースにフローパケットが送出されます。今日のインターネットでは、1 つのフローの平均的な長さは、約 11 パケットで構成されているため、回線が高速なほど、大量のフローレコードとフローパケットを生成できます。

現在、一般的に使用されているフローアカウンティングのパケット形式には、バージョン 5 とバージョン 8 の 2 種類があります。バージョン 5 は、フローごとに送信元と宛先の IP アドレスを 1 つのレコードとして持つ形式のため、アカウンティング用に最適と考えられます。

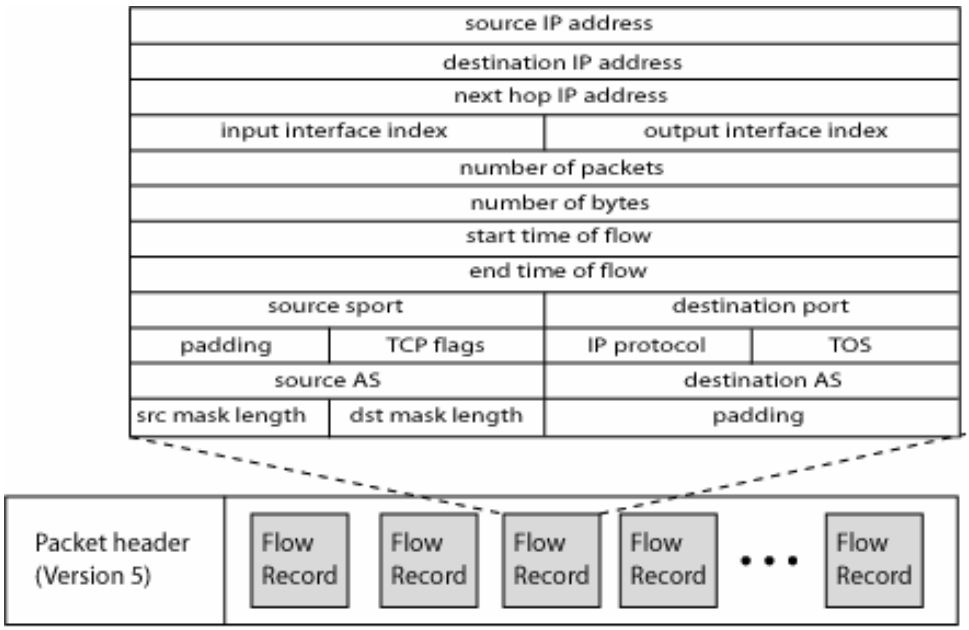

図1：フローアカウンティングバージョン5 のパケット形式

図 1 に示されているように、バージョン 5 のフローアカウンティングパケットには、最初にヘッダがあり、次にフローレコードが続きます。図 2 と図 3 は、ヘッダとフローレコードの形式を示しています。通常、バージョン 5 のフローパケットの場合、フローレコードの数は多くても 30 個で、ほとんどの実装例では、最長 1500 オクテットとなっています。

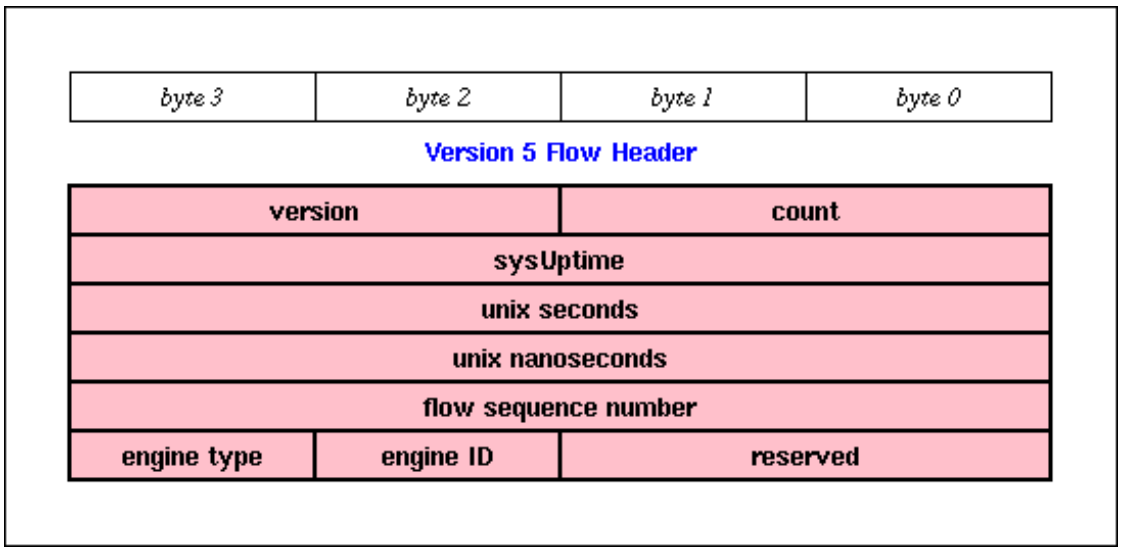

図2：V5 のフローパケットヘッダ形式

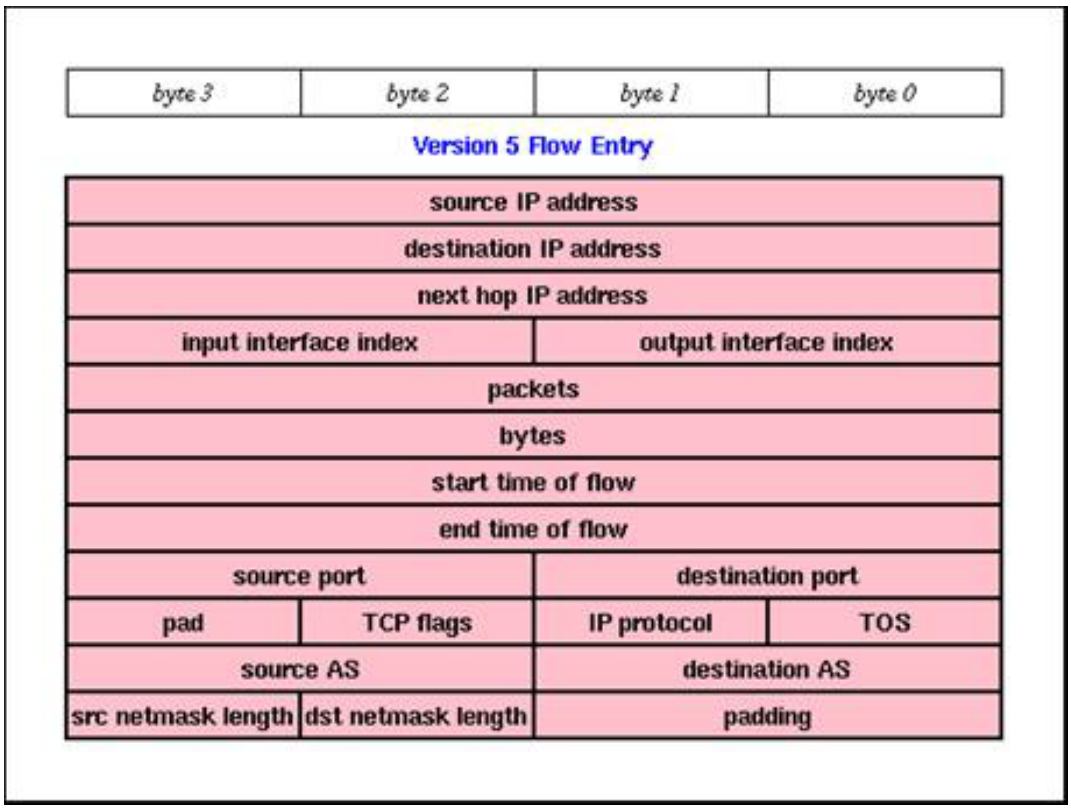

図3 ;V5 のフローエントリ形式

バージョン 8 のフローレコードは、フローの集約が可能です。集約の基準としては、送信元と宛先の自立システム (AS) のプレフィックス、送信元プレフィックス、宛先プレフィックス、宛先プレフィックス/TOS、宛先 AS/TOS、プロトコル/ポートなどが利用できます。フローアカウンティングエンジンが送出するフローバケット数を削減するためには、このような集約方式が必要になります。バージョン 8 のフローレコードは、ネットワーク計画やトラフィックエンジニアリングには有効ですが、ユーザーのアカウンティングにはあまり応用が利きません。

再び V5 のフローレコードの解説に戻りましょう。そもそもフローレコード収集システムは、どのくらいの量のデータを扱うのでしょうか。例として、送受信とも利用率 30%で稼動しているギガビットイーサネット回線のモニタリングを実施するとします。また、平均パケット長は 240 オクテット (イーサネットヘッダを含む) 、1 フロー当たりのパケット数は平均 11 個のごく一般的なインターネットのパケットが流れていると仮定します。このケースでは、フローモニタリングエンジンはおよそ 31 万 2,000 パケット／秒を処理し、約 28,500 個／秒のフローレコードを生成します。生成されたフローレコードは、950 個弱のフローパケット (パケット長は 1464 オクテット) にまとめられます。

つまり、収集システムは 11M ビット／秒をわずかに上回る速度でフローデータを収集・処理し、950 パケット／秒で解析して 28,500 個／秒のフローレコードを処理することになります。これは不可能な作業ではありませんが、小型のマシンで処理できるほど簡単な仕事ではありません。

フローサンプリング

今見てきたように、アカウンティング用のフローモニタリングは、モニタリングエンジンと収集エンジンの双方に大きな負荷がかかります。実際、数万パケット／秒程度のゆっくりしたパケット速度であっても、ルーターにはフローモニタリング専用のハードウェアが必要なため、フローレポーティング実施位置に複数の収集システムを直接接続する方法も考えられます。フローエンジンへの負荷を軽減し、収集システムが複数のフローレポーティングシステムの要求に応えられるようにするには、モニタリング対象となるフローパケットの量そのものを減らす方法があります。つまり、フローのサンプリングです。たとえば、フローレコードを生成するルーターの設定を変更して、実際のパケット処理量の 10%か 1%、場合によっては 0.1%のサンプルを抽出して、ここからフローレコードを生成するのです。

このサンプリング方式の場合、収集したアカウンティング情報の精度は低下します。わずかな誤差がすぐに問題になるわけではありませんが、ある程度の誤差が発生するという事実だけは、はっきりと肝に銘じておきましょう。たとえば、課金システムの場合、99%の信頼区間、誤差±3%の範囲であれば、アカウンティング単位をもっと粗く設定してもかまいません。

あるクラスに属するパケット数推定値の誤差とクラス (例えばユーザー) の総バイト数の分散 (予想される誤差) を推定する方法は、http://www.sflow.org/packetSamplingBasics/index.htm に解説されています。ここでは、その方法を簡単に紹介します。

一定時間中にアカウンティング境界を通過するパケット総数を N.とし、特定クラスに属するパケットの数 (たとえば、特定ユーザーに属するすべてのパケットであるとか、すべての音声系パケットなど) を推定するとします。全パケットのうち、対象クラスに属するパケットの

数を推定するには、まずパケットのサンプル n 個を抽出し、その中で対象クラスに適合するパケット数 c を求めます。これがわかれば、全パケットうち、対象クラスに合致するパケットの総数 N_c は、次の (1) 式で簡単に求めることができます。

$$\bullet\ N_c = \frac{c}{n} \bullet N \tag{1}$$

しかし、この推定値がどの程度の精度なのか知っておく必要があります。推定値の精度を測定するには、推定値 N_c の分散を求めます。周期ごとにパケットをサンプリングすることは、ベルヌーイ試行 (二項試行) の連続と解釈できるため、変数出現数 c は母数 n と母数 p の二項分布に従います。ここで、母数 p は、サンプル抽出率 P と次の (2) 式から推定できます。

$$\bullet\ P = \frac{c}{n} \tag{2}$$

サンプル数が大きいときは、中心極限定理により、サンプル抽出率 P は、漸近的に平均値 p と分散 p(1-p)/n の正規分布にしたがいます。

しかし、今回は推定値 N_c の分散を測定することが目的です。そこで、次の定理が適用できます。ここで、x は確率変数、K は定数とします。

$$\bullet\ VAR(Kx) = K^2 VAR(x) \tag{3}$$

(3) の定理を (1) 式と (2) 式に適用し、さらに正規分布の特性を考慮すると、分散 N_c に次の結果を導くことができます。:

$$\bullet\ \sigma^2 = N^2 \bullet \frac{c \bullet (1 - \frac{c}{n})}{n \bullet (n-1)} \tag{4}$$

この N_c によって推定した場合、対象クラスに属するパケット数は、95%信頼区間で次のように表すことができます。

$$\bullet\ [N_c - 1.96\sigma, N_c + 1.96\sigma] \tag{5}$$

同様に、99%信頼区間では、次のように表されます。

$$\bullet\ [N_c - 2.58\sigma, N_c + 2.58\sigma] \tag{6}$$

上の結果から、推定値 N_c の予想誤差率を導くことができます。今回対象としている分野はアカウンティングであり、基本的に実際の金銭の動きと生身の人間 (ユーザー) が絡むため、99%の信頼区間を採用しました。ここは読者の現場に置き換えて、実際の人間関係や行動などを参考に、適切と思われる信頼区間を設定してください。

$$\bullet\ \%error = 100 \bullet \frac{2.58\sqrt{\mathrm{var}(N_c)}}{N_c} = 100 \bullet \frac{2.58\sqrt{N^2 \frac{c(1-\frac{c}{n})}{n(n-1)}}}{\frac{c}{n} \bullet N} \tag{7}$$

整理すると、

$$\bullet\ \%error = 258 \bullet \sqrt{(\frac{1}{c} - \frac{1}{n}) \bullet (\frac{n}{n-1})} \tag{8}$$

ユーザー数が大量のとき、一般的に n>>c であり、次の近似式が使用できます。

$$\bullet\ \%error \le 258 \bullet \sqrt{\frac{1}{c}} \tag{9}$$

これは非常に興味深い結果です。つまり、ここで得られた誤差率は、サンプリング周期の間に抽出したサンプルのうち、対象クラスに適合するサンプルの数だけに連動して変化するのです。したがって、少なくとも 99%のユーザーを対象に、一定の周期中に受信 (または送信) したパケット数の推定値を 1%未満の誤差に抑えたい場合、ユーザー当たり約 66,000 パケット以上を収集すればよいことに

なります。また、サンプリング実施周期を長くするか、サンプル抽出対象となるトラフィックの割合を増やせば、推定値の精度を高めることができます。

残念ながら、これで終わりというわけにはいきません。今回推定しようとしている量は、対象クラスのパケット数ではなく、対象クラスに適合するトラフィック量です。サンプルとして抽出したフローデータを基に、特定のトラフィッククラスに該当するトラフィック量を推定するとき、実際には次の式を用いて全使用量を推定します。

$$\bullet\ B_c = \overline{b}_c \bullet N_c \qquad (10)$$

ただし、対象クラスのバイト数が B_c、クラス c のパケットの平均パケットサイズが $\overline{b}_c$、サンプルサイズ n での推定です。平均を得るには、個々のサンプルのパケットサイズの総和を求め、サンプル数で割ります。抽出サンプルを用いた測定値の精度を明らかにするには、推定値 B_c の分散を求める必要があります。すでに上記 (4) 式で N_c の分散はわかっています。そこで、$\overline{b}_c$ の分散がわかれば、以下の定理を用いて B_c の分散が推定できます。

$$\bullet\quad \mathrm{var}(XY) = \mathrm{var}(X) \bullet \mathrm{var}(Y) + \overline{X}^2 \bullet \mathrm{var}(Y) + \overline{Y}^2 \bullet \mathrm{var}(X) \qquad (11)$$

b_c の分散 (対象クラスに属するパケットのサイズの長期分散) がわかれば、サンプリング理論を用いて次の答えを得ることができます。

$$\bullet\ \mathrm{var}(\overline{b}_c) = \frac{\mathrm{var}(b_c)}{c} \qquad (12)$$

数学的な説明はこれくらいにとどめますが、注意していただきたいのは、対象クラスのサンプルサイズ c が小さい場合には、サンプリング誤差は非常に大きくなりますが、c が大きい場合には、(11) 式の最初の 2 項は有意性を失い、誤差率は、近似値として示された (9) 式に近づきます。なお、c が大きいと考えられるのは、次の場合です。

$$\bullet\ \frac{\sigma_{\overline{b}_c}}{\overline{b}_c} << 1 \qquad (13)$$

この基準は、対象となるストリームのパケットサイズの分布に大きく依存しますが、最も「現実味」のあるトラフィックストリームであれば、クラスのサンプルサイズは 10,000 パケットで「大きい」と判断できます。

一連の考察から、有効な経験則を導くことができました。この経験則があれば、所定の範囲内の数量推定値の精度を求めたいとき、任意のクラスからどのくらいのパケットを収集すればいいのかがわかります。ここでわかった第 1 の経験則は、パケットサイズの変化によって重大な誤差が生じないように、各クラスから十分なパケット数をサンプル抽出することが大切です。対象となるユーザークラス当たり 10,000 パケットあれば、ほぼ例外なくこの基準を満たすことができます。

第 2 は、もっと大きな誤差への対処です。つまり、対象クラス内のパケット数推定値の誤差が所定の範囲内に収まるように、十分なパケットを収集することが大切です。下の表は、クラスのサンプルサイズのおよその必要量を示しています。ただし、サンプルサイズが 10,000 未満の場合、表では、必要なサンプルサイズを 10,000 とみなしてください。

	ユーザー抽出率(%)と最大誤差率(%)の組み合わせによって、ユーザー1 人当たりの収集すべきパケット数が決まります(パケットサイズは一定と仮定)		
% ユーザー抽出率 / % 誤差率	0.1%	1%	5%
0.1%	10,700,000	6,600,000	3,800,000
1%	107,000	66,000	38,000
5%	4,300	2,660	1,540

表 1 :所定の精度を達成するために抽出すべきサンプルのおよそのパケット数

この表から、高精度をめざすほど、サンプリングインターバルに膨大な量のパケットを収集しなければならないことが一目瞭然です。たとえば、ダウンロード割り当て制限を実施するのに先立って、ユーザーがダウンロードするときのトラフィックを測定し、「1%/1%」(つまりユーザー抽出率1%未満、測定誤差率1%以上) の精度をめざすとします。すると、ユーザー1人当たり最低66,000パケットを収集するまで、割り当て制限は実施できないことになります。ただし、「1%/1%」の精度で66,000パケットを収集する場合、サンプル抽出率は1%ですから、実際にサンプリング周期中に流れるトラフィックは実に660万パケットにもなり、数ギガバイトのデータに相当します。

結論としては、サンプル抽出率が 20%あるいは 10%であれば、多くのユーザーアカウンティングアプリケーションで採用できるはずです。しかし、この割合をもっと高くするのであれば、サンプリング周期を長く取るか、実際の人間関係などの要素を加味して精度要件に自由度を持たせる必要があります。

フローアカウンティングを生かした利用ポリシーの実施

フローアカウンティング自体には、ポリシー実施の機能はありません。しかし、フローアカウンティングがリアルタイムに実行されている以上、フローアカウンティングアプリケーションと制御ゲートウェイの「連動」は不可能ではありません。

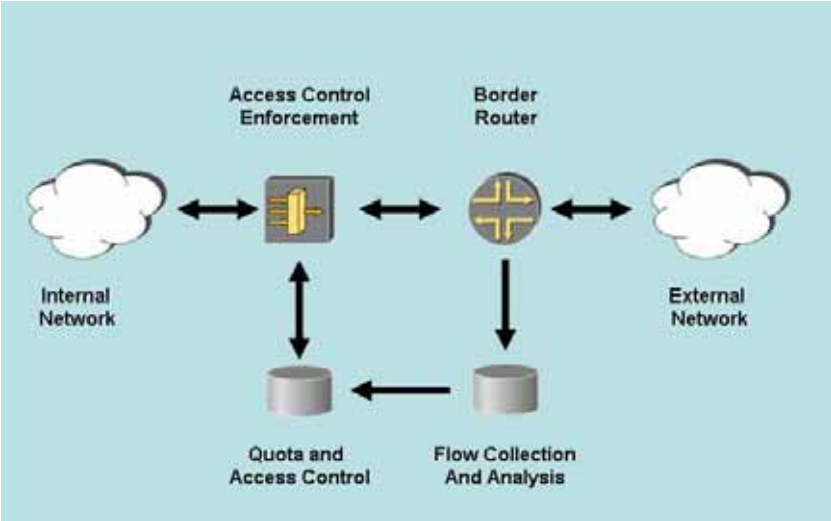

図4：フローアカウンティングを利用したアクセス制御

上の図 4 では、ボーダールーター（またはボーダールーターのすぐ内側に設置されたデータ収集装置）がフローレコードを生成し、集約するためにフロー収集・分析アプリケーションに送ります。通常、このシステムは、レコードを収集し、集約実行後の状態（基準は、内部の IP 番号、外部ネットワークのプレフィックス、AS、課金ゾーンなど）でリアルタイムに割り当て制限・アクセス制御システムに転送します。割り当て制限・アクセス制御システムは、受け取ったアカウンティング情報を組織内部の課金主体（ユーザーや部門など）に対応付けて、記録されている合計値を課金主体に合わせて調整し、課金主体の割り当て制限を超えた場合には、その課金主体のアクセスポリシーを変更します。

通常、アクセス制御を実施するシステムはエッジルーターですが、場合によっては、複数のアプリケーションゲートウェイ（SOCKS ゲートウェイ、HTTP/FTP プロキシなど）を組み合わせることもあります。基本的には、アクセス制御認証を実行するシステムであり、課金主体と各フローの対応関係を確認して、課金主体に対応するアクセス制御ポリシーを実施します。認証に基づいてこうしたポリシーを検索し、実施デバイスにポリシーを渡すのは、割り当て制限・アクセス制御システムの役割です。

このシステムについてじっくりと考察すると、いくつかの重大な問題点が浮かび上がります。

1) どこまで「リアルタイム」のシステムなのか――使用量割り当て制限が適用されている場合、実行可能なアクセス速度に比べて、割り当て量が小さいケースが少なくありません。システムには、フロー情報が集約される場所が 2 つあります。具体的には、ボーダールーターと収集システムです。では、ボーダールーターは、フロー情報を収集システムにいつ流すのでしょうか。たとえば、フローが完了した時点でフローレコードを流すとして、非常に長時間にわたってフローが続く場合、フロー情報が割り当て制限実施システムに到達するころには、割り当て制限を大幅に超過している恐れがあります。フロー収集・分析システムの遅延も考えなければなりません。

2) フロー生成・収集システムの保全性はどのくらい確保されていて、どの程度の比重を占めているのか――ボーダールーターから収集システムへの情報のフローには、信頼性の低い UDP パケット形式が使用されます。通常、ボーダールーターの中で実行されるプロセスの中で、フロー生成プロセスは優先度が低くなります（そもそも、ボーダールーターの本分はパケット転送とルーティング情報の処理なのです）。そのため、突然、トラフィックのバーストやいわゆる経路のぱたつきが発生した場合、ボーダールーターのアーキテクチャにもよりますが、フロー情報が生成されない可能性もあります。また、フロー情報のバーストが発生すると、一時的に収集システムが過負荷状態に陥りかねません。このような事態が併発でもすれば、アカウンティング情報の保全性と精度が損なわれることになります。

3) どの程度の拡張性があるのか――トラフィック量とフローデータ量は線形関係にあります。40k パケット／秒（40kpps）で処理できるシステムは、1Mpps では実行できません。また、このようなシステムを使用する場合、ボーダールーターは、本来の仕事であるパケットのルーティング機能とは関係のないフローデータ生成機能の影響で、スループットが制限されてしまうのです。

サービスゲートウェイによる制御・アカウンティング

フローによる制御に取って代わる選択肢として、サービスゲートウェイを利用する方法があります。この方法の原型は、キャリアのブロードバンドアクセスネットワークにあります。この手のシステムの典型的な構成図が図 5 です。この方法では、アカウンティング機能とアクセス制御機能がサービスゲートウェイに集中するため、ボーダールーターは本来の仕事であるルーティングに専念できます。

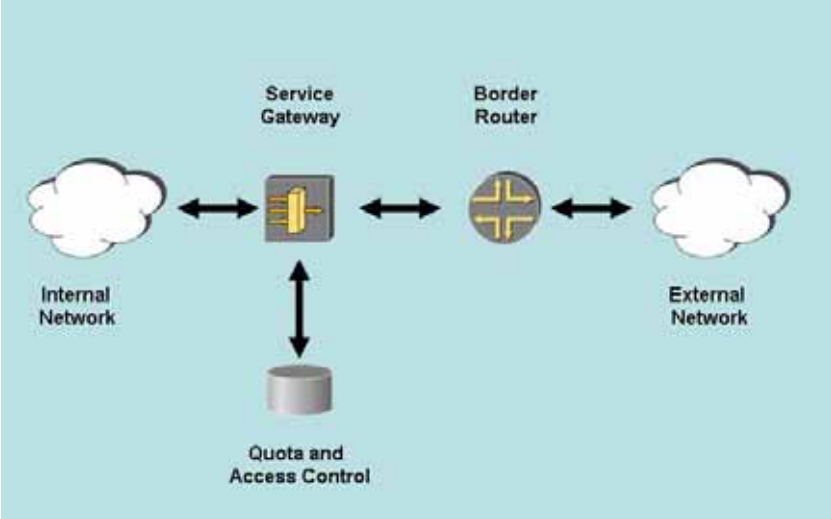

図 5：サービスゲートウェイによるアカウンティング・制御

この環境では、外部へアクセスしようとすると、サービスゲートウェイがいったん遮断し、割り当て制限・アクセス制御システムとユーザーの間の認証交換が実行されます。このアクセス制御交換の実行方法としては、ウェブポータル経由や、ネットワーク全体のシングルサインオン方式（Windows のサインオンなど）があり、両方を組み合わせることも可能です。

アカウンティング情報は、サービスゲートウェイから割り当て制限・アクセス制御システムに送られます。割り当て制限・アクセス制御システムは、利用状況を追跡管理し、使用量がしきい値を超えた場合には、その場でポリシーを変更します。アカウンティング情報の転送は、いくつかの方法があります。第 1 は、フローレコードの形を取るもので、基本的には前述のフローアカウンティングの方法と同じですが、ボーダールーターが持っていたアカウンティング機能はサービスゲートウェイ側に移っている点が異なります。前述の問題点は依然として残っています。ただし、アカウンティングの拡張とボーダールーターの拡張は連動していません。

第 2 は、RADIUS の暫定的なアカウンティングレコードを利用する方法です。サービスゲートウェイにはフローごとの課金主体情報が存在するため、IP フローではなく課金主体を基準にしたレコードをアカウンティングシステムに送ることができるのです。この方法であれば、アカウンティングのトラフィックと収集システムへの負荷が大幅に軽減されます。また、RADIUS は信頼性の高い独自のプロトコルのため、RADIUS の暫定更新情報が失われないように保護対策が取られており、アカウンティング情報の保全性も確保されます。それと引き換えに、一部の詳細情報（送信元・宛先 AS、TOS など）は失われる恐れがあります。さらに大きな問題として、暫定アカウンティングレコードの更新間隔が挙げられます。割り当て制限追跡管理システムが的確に機能するためには、暫定アカウンティング情報の更新を待つ間にユーザーの割り当て制限が空白状態にならないように、暫定アカウンティング情報をユーザーに頻繁に転送する必要があります。つまり、サービスゲートウェイは、RADIUS の暫定更新情報を各ユーザーに 1 分おきか 2 分おきに送る必要があるのです。ある時間内に何千ものユーザーがログオンした場合、サービスゲートウェイと割り当て制限管理システムに大きな負荷がかかることになります。

第 3 の方法としては、アクティブポーリングが挙げられます。認証イベント後、認証システムがユーザーポリシーを適用する際に、いくつかの機能がセットアップされます。具体的には、そのユーザーつまり課金主体へのアクセスを管理するフィルタや、システム内に定義されているサービス（トラフィックがオンネットかオフネットか、ウェブトラフィックがプロキシ経由か非経由かなど）ごとに使用量を追跡管理するカウンタなどです。割り当て制限管理システムは、どのユーザーがログイン中で、ユーザーごとにどのカウンタが対応しているのか把握しています。しかも、ユーザーの現在の割り当て状態までもわかっているのです。したがって、サービスゲートウェイのアクティブポーリングをシステム内のユーザー向けに実行できるというわけです。さらに、ユーザーの割り当て状況に合わせて、ポーリング間隔を調整することも可能です。すでに割り当てがなくなったユーザーの場合、ポーリング頻度は非常に少なくなります。逆に、割り当てがたくさん残っているユーザーには、ポーリングを 15 分おきといった頻度で実行できます。割り当て限度に近づいているユーザーには、30 秒～1 分おきといった頻度でポーリングを設定できます。

使用するポーリング方式は、割り当て制限管理システムやサービスゲートウェイの設計によって異なります。リソースの有効利用やデータ保全性を考えると、COPS や COPS-PR など、高信頼で長期接続が可能な方式が望ましいのですが、SNMP を使っても同じ結果を得ることができます。

サービスゲートウェイをベースにアカウンティング・制御システムを設計する場合、重大な問題がいくつか考えられます（場合によっては、フローベースのシステムでも同じ問題がありえます）。

4) ユーザーが割り当て制限を超えるとどうなるのか――即座にアクセス権停止措置を取るポリシーの場合、たとえば 1GB のデータを 900MB までダウンロードしたところで、アクセス権が突然停止されてしまうと、ユーザーはデータをすべて失うことになります。そのような目に遭ったユーザーは到底納得がいきません。そこで考えられる方式としては、新規の接続を拒否するものの、割り当て制限を超える前から続いているセッションは、制限を超えても条件付きで認めるというものです。たとえば、割り当て量の「借り越し」を一定範囲で用意します。また、割り当て制限に近づいたり、超過したりした場合に接続速度を制限する方法もあります。

5) サービスゲートウェイでのログインの永続性（パーシステンス機能）はあるのか――たびたび再認証を求められるようではユーザーも閉口しますが、かといって、共用のワークステーションでサービスを利用して席を離れた後で、自分の割り当て制限を他のユーザーに勝手に使われてしまうのも考えものです。これまでの経験から言って、タイムアウト型のシステムに統一してしまうと、一部のユーザーから不満が出ます。現在、広く普及しているシステムでは、サービスゲートウェイとユーザーのワークステーションの間で、永続的な TCP 接続を維持する方式が取られています。通常、HTTP 接続で、必要に応じてブラウザ側のウィンドウに現在の使用量、残りの割り当て量などの情報を表示します。ブラウザ側のウィンドウを閉じればセッションが終了するため、安心して端末を離れることができます。

6) 何はなくとも拡張性が重要。ゲートウェイは同時セッション数をいくつまでサポートするのか。割り当て制限管理・認証用のサーバには、どの程度の規模のシステムが必要か――このタイプのシステムであれば、大規模ネットワークにサービスゲートウェイを分散配置できるため、拡張性の不安はある程度軽減されます。ネットワークを小分けにして各ゲートウェイに管理させる形態のため、ネットワーク利用状況に合わせて、系統立てた拡張が可能です。ただし、分散配置する装置が専用のサービスゲートウェイではなく、ボーダールーターとフロー収集システムの組み合わせの場合、この方式は非常に困難になります。サービスゲートウェイは大規模なブロードバンドアクセス用インフラでの使用を前提に設計されているのが一般的です（例外もあります）。そのため、分散配置を検討する前に、まず大規模なネットワークを整備する必要があります。

7) 精度と保全性の問題。サービスゲートウェイは、そもそもサービスゲートウェイとして設計されたものなのか、それともサービスゲートウェイ機能が「おまけ」で付いているエッジルーターなのか。エッジルーターにある MIB 情報へのポーリングでアカウンティング情報が得られるとしても、この MIB 情報はどの程度の精度なのか――こうした基準によって、メリットは大幅に異なります。

ワイヤリングクローゼットでの制御・アカウンティング

組織の都合によっては、ユーザーのトラフィックの送信元の近くに制御機能を置きたい場合もあります。つまり、アクセス制御を外部ネットワークとのボーダーに置くのではなく、ワイヤリングクローゼット内やユーザーのアクセス環境に置くという考え方です。たとえば、大規模ネットワークに次々に登場している無線 LAN は典型例と言えます。また、教育機関などに見られる共用端末や共用 LAN ポートも代表的な例です。いずれも、組織として、ネットワークへのアクセスを認証ユーザーに限定する目的があります。

このニーズに応えるために最近増えている方法は、802.1x に RADIUS かドメインログインを連携させて、ネットワークに接続するユーザーを認証する形態です。ホストのオペレーティングシステムは必ずしも 802.1x（別名 EAPOL）をサポートしているわけではないため、オプションとしてウェブベースの認証も許可されているケースが大半です。ユーザー認証前の時点では、デフォルトのアクセス権限は、ウェブポータルへのアクセスに限定されています。

LAN 認証については、本ホワイトペーパーのテーマから外れますが、関連事項だけ簡単に触れておきます。ワイヤリングクローゼットのアクセススイッチは、アカウンティング・制御システムのアカウンティングゲートウェイとして利用するには機能不足の観がありますが、ウェブポータルか 802.1x を通して認証されたユーザーにとっては、外部からネットワークにアクセスする際に再認証の手間が省けるため便利かもしれません。トラフィック量追跡管理と認証のシステムは、シングルサインオンを前提に設計することが大切です。

結びにかえて

本ホワイトペーパーでは、大規模組織のネットワークに外部からアクセスする状況を想定し、アカウンティングや制御に伴う課題と解決策をいくつか解説しました。今や、どのような組織を運営する場合でも、インターネットアクセスとオンネット VPN アクセスは必須となっており、年度予算の重要な一角を占める存在となっています。そうした状況を踏まえた総合的なネットワーク管理戦略の中では、アカウンティングと制御はほんの一部の要素に過ぎません。ほかにも、課金システム、認証システム、ポリシーデータベース、ネットワークモニタリングシステムなど、本ホワイトペーパーでは別テーマのために触れられなかった要素がいくつもあります。いずれも、総合的なネットワーク管理戦略には不可欠の要素です。今回取り上げたシステムは、スタンドアロンのシステムと見ることもできますが、導入効果を最大限に引き出すためには、今挙げたような各種システムと連携させる必要があります。

とはいえ、アカウンティング・制御システムの単独利用も、十分検討に値することは明白です。以下に要点をまとめました。

- 使用量のアカウンティングとポリシー制御のシステムがない組織の場合、リソースの乱用・無駄遣いに陥りがちです。どうしてもリソースの無駄遣いや非効率的な利用は避けられません。最悪の場合、リソースの不正利用が発生するだけでなく、リソース乱用が引き起こす事件・事態への組織的な責任問題にも発展しかねません。電話

利用を課金・記録しなかったり、乱用され放題になっていたりする組織はありえませんが、ネットワークは野放しという組織が少なくないのです。

- 使用量のアカウンティング情報を課金システムに送り、リソース利用に応じてユーザーまたは所属部門に課金――。この流れを確立することが、ネットワークのリソース利用に対する適切な予算編成の基盤となるのです。
- 通常、大規模組織での使用量のアカウンティングには、フローアカウンティングかサービスゲートウェイによるアカウンティングが使われています。
- フローアカウンティングは、最も古くから使われており、多くのネットワークデバイスに「無償」で搭載されているため、導入も非常に簡単とされています。しかし、ネットワーク構成要素やフローデータ収集デバイスに大きな負荷がかかるなど、拡張性の問題があります。
- フローアカウンティングでの拡張性の問題は、サンプル抽出対象をパケットフローの一部に限定することで、ある程度解消できます。しかし、この対処方法では、対象となる課金主体が個人ユーザーの場合、精度が大きく低下する恐れがあります。実際にビジネスが絡むと、このような甘い精度では通用しません。さらに、広帯域の回線の場合、一部のベンダの製品の仕様では間に合わないほどのスピードで、サンプルを抽出する必要も出てきます。
- サービスゲートウェイによるアカウンティングは、認証、アクセス制御、アカウンティングを単一の専用ハードウェアにまとめ、割り当て制限・アクセス管理システムから制御します。アクセス制御・割り当て制限システムにデバイスやシステムをいくつも使用しないため、フローベースのアカウンティングシステムに比べて、設備投資や運用コストの削減につながり、信頼性もアップします。
- サービスゲートウェイによるアカウンティングシステムは、アカウンティングとユーザー制御を 1 台のサービスゲートウェイで処理するため、カウンタベースのアカウンティングと親和性が高く、サンプル抽出も不要です。
- 割り当て制限やアカウンティングにどの手法を使う場合でも、以下の事項について必ず考慮しておく必要があります。
  - どこまで「リアルタイム」のシステムなのか。アカウンティング情報が割り当て制限管理システムに届くのが遅延したために、システムの対応が遅くなり、結果的にユーザーが割り当て制限を大幅に超過するような事態はないのか。
  - システムの拡張性はどうか。現在、50M ビット／秒のスループットで問題ないとしても、将来、10G ビット／秒に増強可能か。現在、1,000 ユーザーの同時ログインに対応できていても、将来 10,000 ユーザーを処理できるか。アップグレードパスが用意されているか。
  - アカウンティングの精度はどうか。組織や経理部門が求める精度要件を満たしているか。
  - システムの柔軟性はどうか。宛先ネットワーク、送信元ユーザー、アプリケーションタイプ、QoS 属性などを基準にしたアカウンティングをサポートしているか。
  - ユーザーやポリシーのデータベース、課金システムなど、既存の OSS（運用支援システム）への統合作業は簡単か。

コンポーネントの選定や、ユーザーアクセス制御・割り当て制限管理システムの設計に当たって、ここに挙げた事項をすべて考慮に入れてシステム構築を進めれば、導入当初だけでなく、将来的にも納得のいくパフォーマンスが得られるのです。

米国本社
Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
電話408-745-2000
FAX 408-745-2100
www.juniper.net

アジアパシフィック
Juniper Networks (Hong Kong) Ltd.
Suite 2507-11, Asia Pacific Finance Tower
Citybank Plaza, 3 Garden Road
Central, Hong Kong
電話852-2332-3636
FAX 852-2574-7803

ヨーロッパ、中東、アフリカ
Juniper Networks (UK) Limited
Juniper House
Guildford Road
Leatherhead
Surrey, KT22 9JH, U.K.
電話44 (0) -1372-385500
FAX 44 (0) -1372-385501

日本
ジュニパーネットワークス株式会社
東京本社
〒163-1035 新宿区西新宿3-7-1
新宿パークタワーN棟35階
電話03-5321-2600/FAX 03-5321-2700
西日本事務所
〒541-0054 大阪市中央区南本町3-5-3-708
電話06-6281-6166/FAX 06-6281-6166
URL http://www.juniper.co.jp