お客様各位

東京都港区芝浦 4-2-8
株式会社 UCOM

「uRPF」技術についてのご説明資料

【uRPF 採用の背景】

昨今、ワームやボットに感染し、DDoS 攻撃など不正通信の踏み台とされるケースが増えてきています。乗っ取られた数多くの PC から発信される Smurf 攻撃、SYN flood 攻撃や ICMP flood 攻撃などでは、踏み台とされた PC の IP アドレスではなく、偽装された IP アドレスが送信元 IP アドレスに使われることが増加しており、発信源の特定と対策を困難なものにしています。このような不正で不要な通信が大量に発生すると、お客様のネットワークや ISP のバックボーンに多大な負荷がかかり、正常な通信を阻害してしまいます。UCOM では、このような不正なトラフィックからお客様の環境とバックボーンを守るために、uRPF 機能の全面的な採用を進めております。

【uRPF とは】

「unicast Reverse Path Forwarding」の略で、ルータのルーティングの仕組みを使ったパケット・フィルタリング技術です。IP ネットワークでトラフィックの中継を担うルータは、受信したトラフィックの宛先 IP アドレスを検出し、自身のルーティングテーブル（経路情報）から宛先 IP アドレスが存在するインタフェース (IF) を割り出し、適切に転送することを実行しています。uRPF は、このルーティング・メカニズムを応用した機能で、送信元 IP アドレスと経路情報を照らし合わせ、本来の経路を辿って来たトラフィックか否かをチェックします。ルーティングテーブルに無い IP アドレスが、IP ヘッダの送信元 IP アドレス部に記載されているトラフィックを発見した場合はフィルタリングされて破棄されます。これによって不正な IP アドレスや詐称された IP アドレスを送信元とするトラフィックが、他へ伝播することを防ぐことが可能となります。

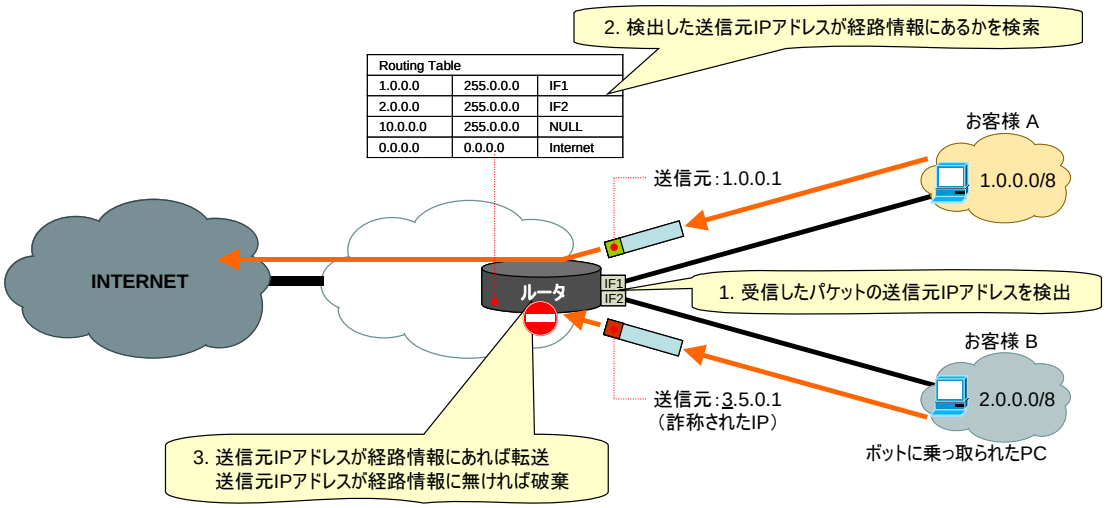

図 1 uRPF の動作概念

uRPF には、「strict」モードと「loose」モードの 2 つの動作モードがあります。

- **厳密な strict モード**
  検査するトラフィックの送信元 IP アドレスがルーティングテーブルに載っており、かつ、受信したルータのインタフェースの先に送信元 IP アドレスのネットワークが存在するかどうかをチェックします。ルーティングテーブルに存在しない IP の場合や受信インタフェースが異なる場合、トラフィックはフィルタリングされ破棄されます。厳格なチェックを行うので、すべての IP 詐称の検出が可能です。一般にお客様を収納するルータのポートに設定されます。

- **緩やかな loose モード**
  検査するトラフィックの送信元 IP アドレスがルーティングテーブルに載っているかだけをチェックします。ルーティングテーブルに存在しない場合、トラフィックはフィルタリングされ破棄されます。緩やかなチェックを行うので、実在する IP アドレスを詐称された場合は検出することができません。一般に他の ISP 間の相互接続ルータに設定されます。

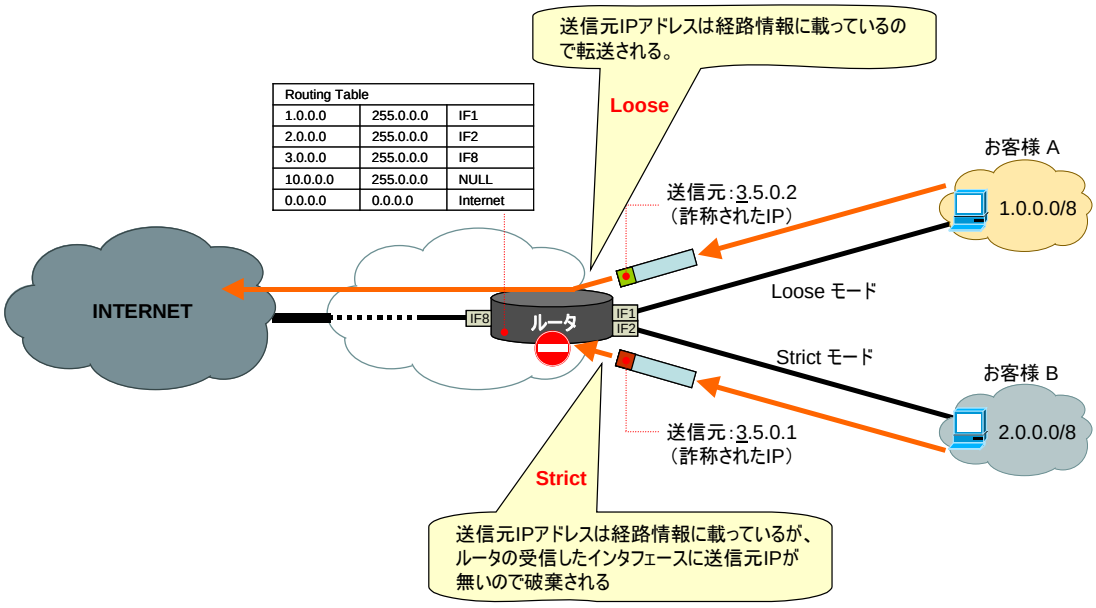

図 2　uRPF の strict モードと loose モード

【uRPF の適用】

UCOM では、他 ISP との相互接続点（POI）のルータインタフェースに対し、uRPF loose モードを既に設定しています。これにより他 ISP 網内を発信源とする不正な送信元 IP アドレスを持つトラフィックを遮断し、UCOM 網全体を外部からの不正トラフィックから守っています。

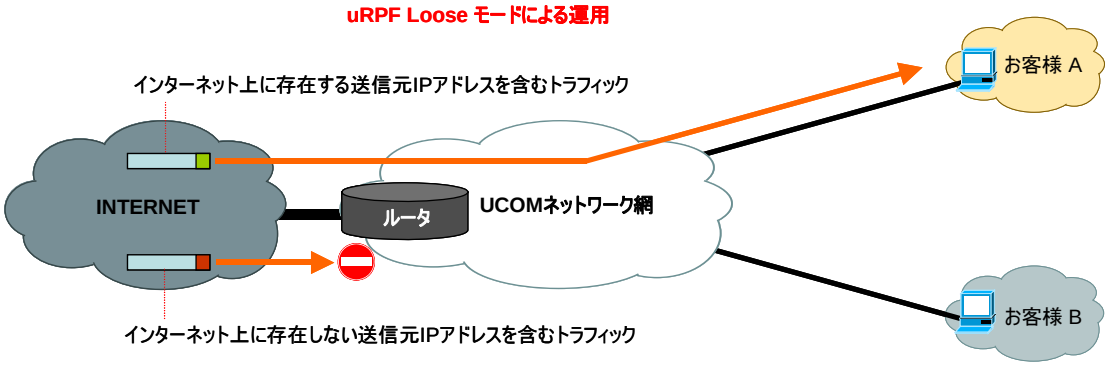

図 3　UCOM 網へ外部からの詐称トラフィックの侵入を排除

BROADGATE 02 光トランジットアクセス[注1]を除くすべてのサービスに対してuRPF strictモードを設定していきます。これにより、お客様のコンピュータなどが万一ボットなどに感染し、お客様の意図に反してDDoS攻撃の加害者になってしまうことを防ぎます。

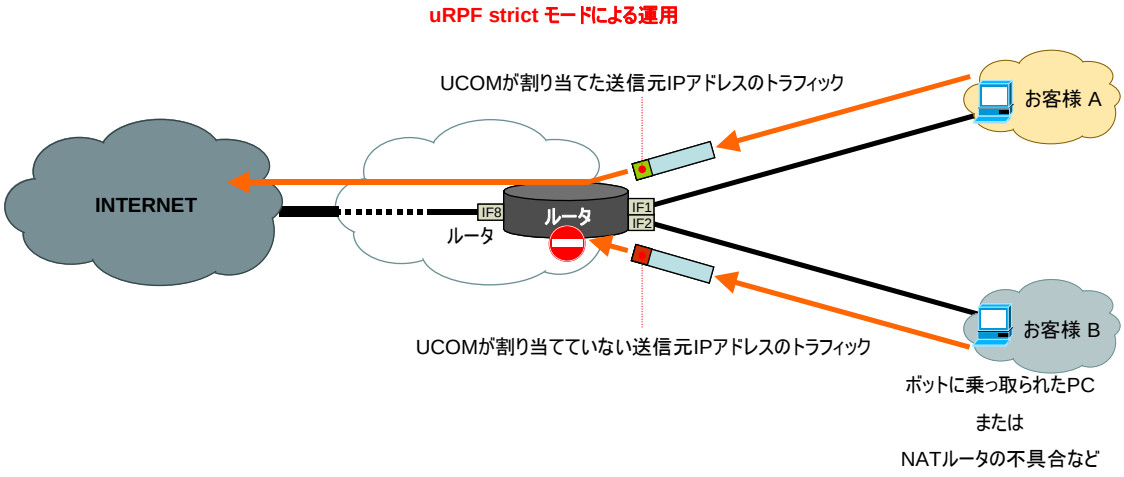

図 4　UCOM 網へのアクセス部分で詐称トラフィックの侵入を排除

【通信への影響】

お客様の回線を収容する UCOM 機器で厳密な uRPF strict モードを適用すると、UCOM が割り当てた IP アドレス空間を送信元にしたトラフィックのみが正常な通信とみなされます。UCOM が割り当てた以外の IP アドレスを送信元とするトラフィックはすべてフィルタリングされて破棄されてしまいます。もちろん通常のお客様や正しくルータを設定されているお客様の通信にはまったく影響ありません。

Strict モードを適用した後に稀に通信不能になるケースがありますが、第一の原因としてお客様がお使いのルータやソフトウェアの不具合が考えられます。例えば UCOM が割り当てた以外の IP アドレスが使われてしまう場合や、ルータの NAT 機能の不具合あるいは設定漏れが原因でプライベート IP アドレスのまま転送されてしまう場合です。このような場合は、ご利用中のネットワーク機器などの設定を再度ご確認されるようお願いいたします。

それ以外にネットワーク構成が原因で、uRPF フィルタによって通信が不能になるケースがいくつか考えられます。

ケースA ： 1 台のサーバを複数の回線に接続したケース

[現象] A 社では、インターネット回線として UCOM1 と UCOM2 (または ISP-A) を契約しており、サーバを各 ISP のセグメントに接続して外部に公開しています。ところが、インターネットユーザ (3.3.3.3) から UCOM1 側の IF (1.0.0.2) にはアクセスできますが、UCOM2 側の IF (2.0.0.2) にアクセスすることができません。

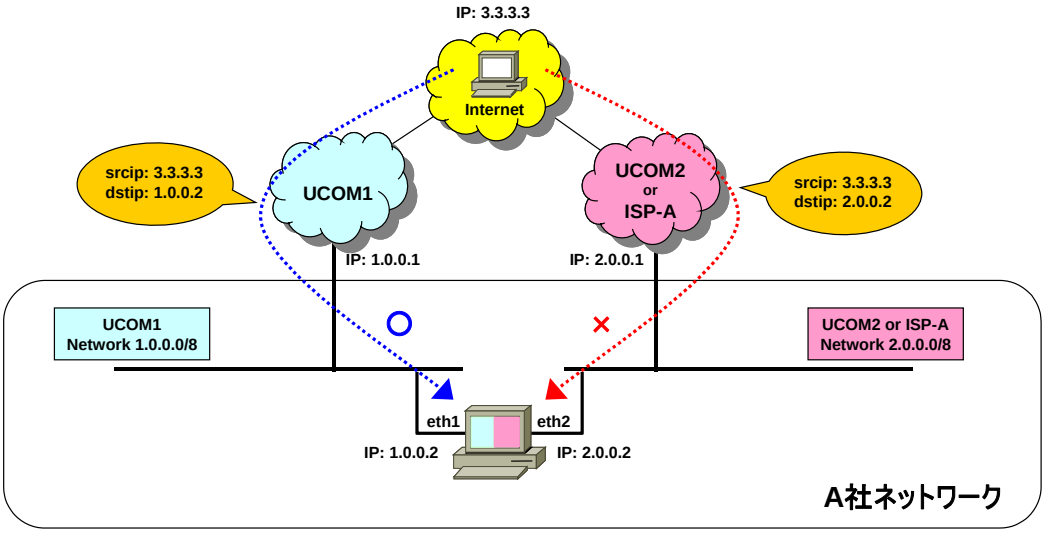

図 5 1 台のサーバを複数の回線に接続したケース (現象)

[原因] クライアントからのリクエストパケットに対してサーバが応答パケットを送信する場合、必ずしもそのリクエストパケットを受信した IF から送信されるわけではありません。通常、サーバは自身に設定されているデフォルト GW アドレスを参照してパケットを送信します。そのため、図 6 のケースでは、eth2 宛のリクエストパケットに対する応答は、デフォルト GW が設定されている eth1 側の IF から送信されます。これにより、UCOM2 側の IP がソースとなったパケットが UCOM1 側に流れてしまうため、uRPF フィルタによって破棄されてしまいます。回線ごとにサーバを分ける、あるいはサーバにポリシールーティングの設定を行うなどの対策が考えられます。

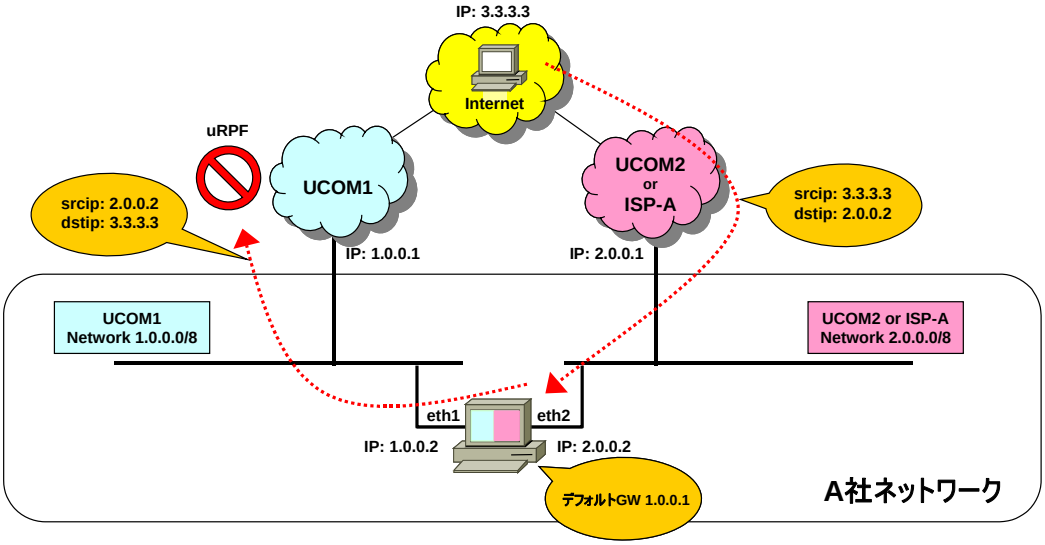

図 6　1 台のサーバを複数の回線に接続したケース　(原因)

ケースB ：　ルータで異なる回線間のセグメントを接続したケース

[現象]　B 社では、インターネット回線として UCOM1 と UCOM2 (または ISP-A) を契約しており、二つのセグメントをルータで接続しています。通常、UCOM2 のユーザは、デフォルト GW を 2.0.0.1 に設定して UCOM2 を利用していますが、最近 UCOM2 のトラフィックが多くなってきたため、一部のユーザのみデフォルト GW を 2.0.0.10 に変更して、UCOM1 経由で通信を行う予定です。しかし、実際に切り替えてみたところ UCOM1 経由でインターネットにアクセスすることができません。

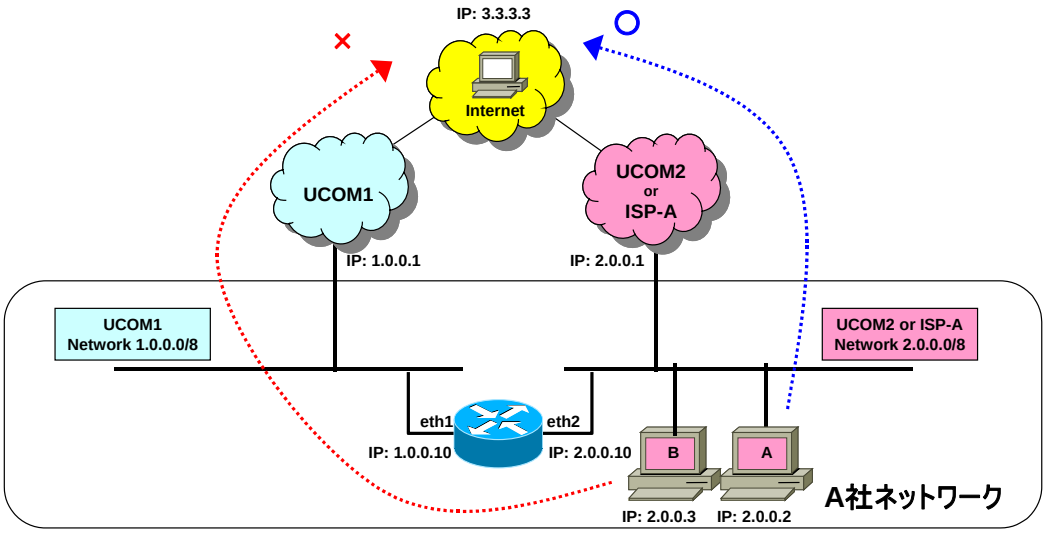

図 7　ルータで異なる回線間のセグメントを接続したケース (現象)

[原因]　IP パケットは、ルータを経由しても IP アドレスが変更されないことに注意してください。このケースでは、UCOM2 側の IP がソースアドレスとなったパケットが UCOM1 側に流れてしまうため、uRPF フィルタにより破棄されています。ユーザのセグメントを移動して IP アドレスを変える、あるいはルータで NAT を設定するなどの対策が考えられます。

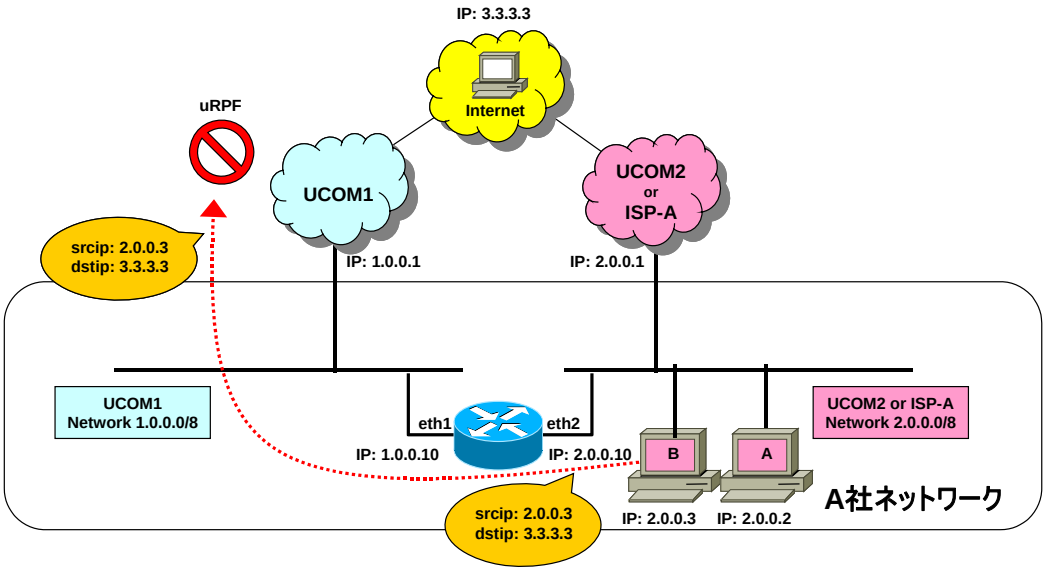

図 8　ルータで異なる回線間のセグメントを接続したケース (原因)

ケースC ：　2 回線を同一スイッチに収容したケース

[現象]　C 社では、UCOM 回線を 2 回線契約しており、どちらの回線も同じスイッチに収容しています。ところが、すべてのユーザ通信が不安定で、タイミングによっては全く通信することができません。

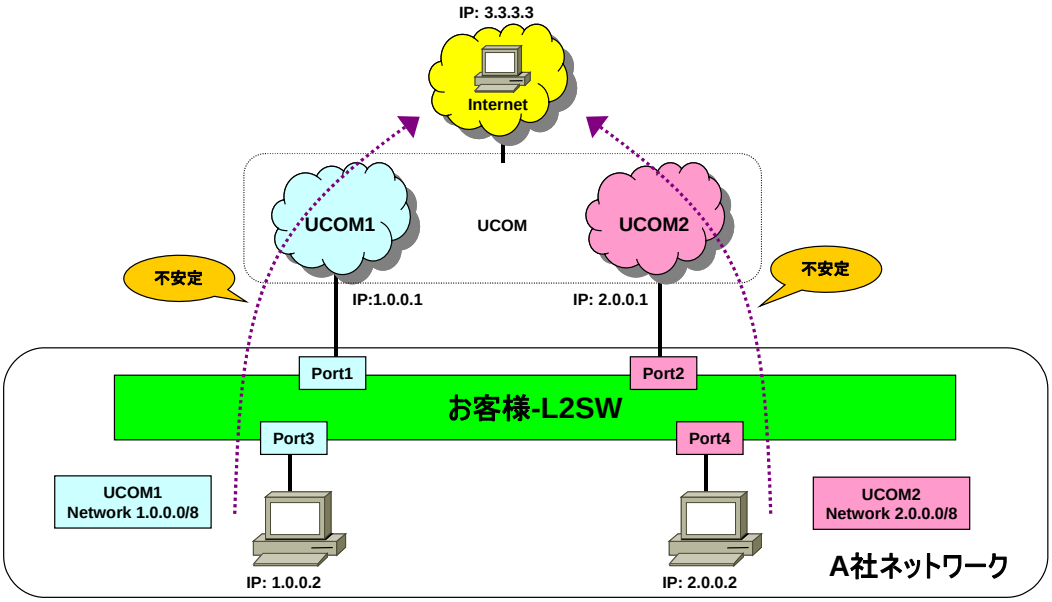

図 9　2 回線を同一スイッチに収容したケース (現象)

[原因]　UCOM の同一収容機器 (UCOM-L3SW) から提供される回線を 2 本利用している場合、基本的に UCOM 側 IF は 2 回線とも同じ MAC アドレスを持っています。この 2 回線をお客様側で同一のスイッチングハブ (お客様-L2SW) に収容した場合、同一 MAC アドレスの機器がスイッチングハブの複数のポートに同時接続されていることになるため、MAC アドレスの学習ポートが頻繁に変更されてしまいます。その結果、速度遅延やパケットロスなどが発生する可能性があります。また、スイッチングハブによっては CPU 負荷が高くなり、リブートなどを引き起こす可能性もあります。さらにこのケースでは、タイミングによって MAC アドレスがどちらのポートに学習されているかわからないため、正しくない回線にパケットが流れてしまった場合には、uRPF フィルタにより破棄されてしまいます。お客様-L2SW を 2 台に分割する、あるいはお客様-L2SW に VLAN を設定して論理的に 2 台に分割するなどの対策が考えられます。

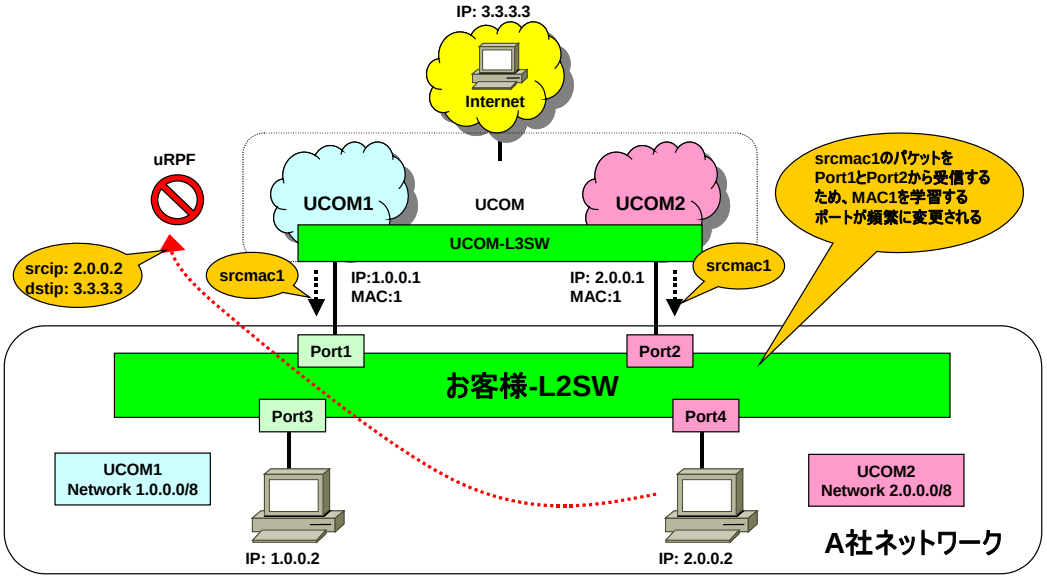

図 10　2 回線を同一スイッチに収容したケース (原因)

以上

注 1 ： BROADGATE 02 光トランジットアクセスでは、uRPF を利用するのではなく、お客様から申請のあった経路情報を送信元 IP アドレスとするトラフィックのみを受信する ACL（Access Control List）を設定して、送信元アドレス検証を実施しています。