ケーブル技術スタッフの機器チェック!

日々開発されるケーブルテレビ関連機器を、技術スタッフが厳しい目でチェック! 実用性に焦点を当てて報告します。

No. 57

OP25B

豊島ケーブルネットワーク(株) 技術部 部長　上山裕史

今回はスパムメール送出対策として、
OP25Bの外部接続ルータへの設定について紹介します。

私たちケーブルテレビ局の技術者はISP(インターネット・サービス・プロバイダ)として顧客のセキュリティや、自ネットワークからの不正パケットの送出を防ぐために不断の努力をしています。今回はスパム(迷惑)メール送出対策として、OP25Bの外部接続ルータへの設定を紹介します。

OP25Bは、Outbound Port 25 Blockingの略です。ウィルスなど悪意のあるプログラムを実行できる顧客のPCが送る不特定多数宛のメールをブロックするのが目的です。フィッシング詐欺や迷惑メールなど犯罪と直結する場合が数多くあるので、見知らぬ外国のネットワーク管理者やセキュリティ団体から、迷惑メールを止めるよう要請するメールが突然入ってきます。この警告を放置しておくと、オープンリゾルバと同じで迷惑メールや不正パケットを出し続けるISPは、特に欧米の大手ISPからは設備を損壊する恐れのあるものとして、入り口でパケットを遮断される可能性があります。そうなればユーザからメールが届かない、Web閲覧ができないといったクレームが出てきます。

また、疎通を回復するために英語で膨大なやり取りをした上、自社設備の防止設定をすることが再開の条件であったりします。常に自ネットワークをクリーンに保つようにすることで、このような事態を回避できます。OP25Bを実施済みと宣言しているケーブル局でも、次のURL(http://www.senderbase.org/)の右上にドメインを入れて検索すると、多くのスパム送出アドレスが出てきます。検索は簡単ですので、OP25Bの設定が正しいか見直すことができます。図1に確認サイトの概要を示します。

図2はスパム送信をユーザPCが直接外部に向けてできないように設定する、外部接続ルータ向けコンフィグを示します。このルータのインターフェースに図3のような設定を入れます。このアクセスリストでは、permitコマンドで自ネットワークのIPアドレスを指定し、smtp(メール送信ポート番号25)を拒否し、ログを取るように指示しています。自ネットワークのIPアドレスは202.xxx.yyy.0としています。時々ログをチェックすると、自社ユーザでウィルスに罹っている確率の高いPC(パソコン)を発見できます。

地域密着のISPの利点である顧客とのコミュニケーションの近さで、PCからウィルスの除去をしてあげることで、さらにユーザの信頼を得ることができます。ウィルスは悪質でユーザPCに電源が入っていれば、裏で黙々と迷惑メールを送信し続けるのです。

ケーブル局の技術者はメールサーバやWWWサーバのアウトソーシング化で、インターネットの知識が不要になることは無く、顧客へのサービス品質を上げるために自ネットワークのクリーン化を進めると同時に、ますますインターネットの知識が必要になっていくと考えます。

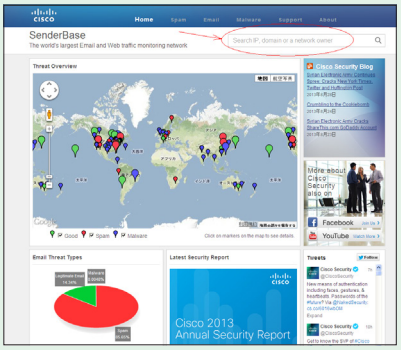

図1:確認サイトの概要

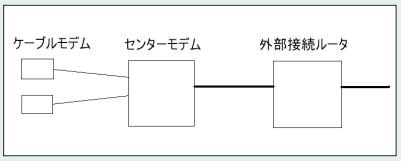

図2:外部接続ルータ向けコンフィグ

```
<設定箇所>
interface GigabitEthernet1/1
 ip access-group OP25B out                    ※適用

<設定内容>
ip access-list extended OP25B
 permit tcp 202.xxx.yyy.0 0.0.0.255 any eq smtp
 deny tcp any any eq smtp log                 ←smtp(25番)を遮断
 permit ip any any                            ←SMTP(25番)以外を許可
```
図3:設定するルータ