Topic

平成 25 年 9月 6日

SIP サーバの探索と考えられるアクセス増加の注意喚起について

宛先ポート 5060/UDP に対するアクセスが再び増加しています。

1 概要について

警察庁においては、IP電話機などで使用されている通信プロトコル SIP[1]で利用されている 5060/UDP に対するアクセスの増加を検知しています。同ポートに対するアクセスは平成 22 年7月に急激な増加を検知[2]した後、一定の水準で推移していたためアクセスの動向に注視していましたが、平成 24 年 11 月頃から再び増加しています(図 1)。

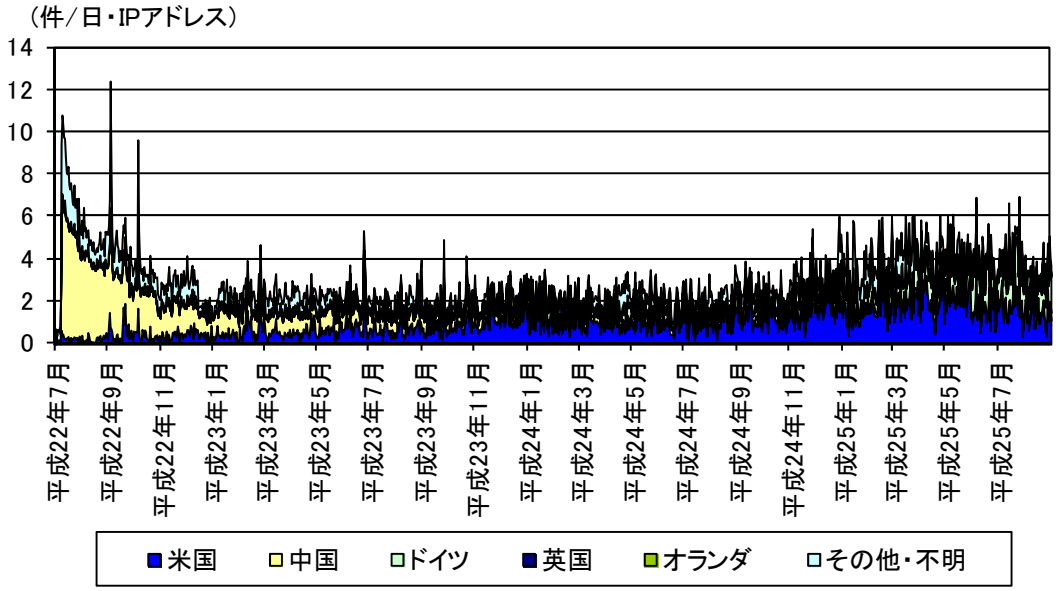

図 1 宛先ポート 5060/UDP に対するアクセス件数の推移(H22.7.1～H25. 8. 31)

[1] 音声データをインターネット上で送受信する技術を VoIP(Voice over Internet Protocol)と言います。SIP(Session Initiation Protocol)は、VoIP で使用されるプロトコルで発信、着信、応答、切断といった制御を行います。

[2] 5060/UDP に対するアクセスの増加について(平成 22 年7月 14 日)
http://www.npa.go.jp/cyberpolice/detect/pdf/20100714.pdf

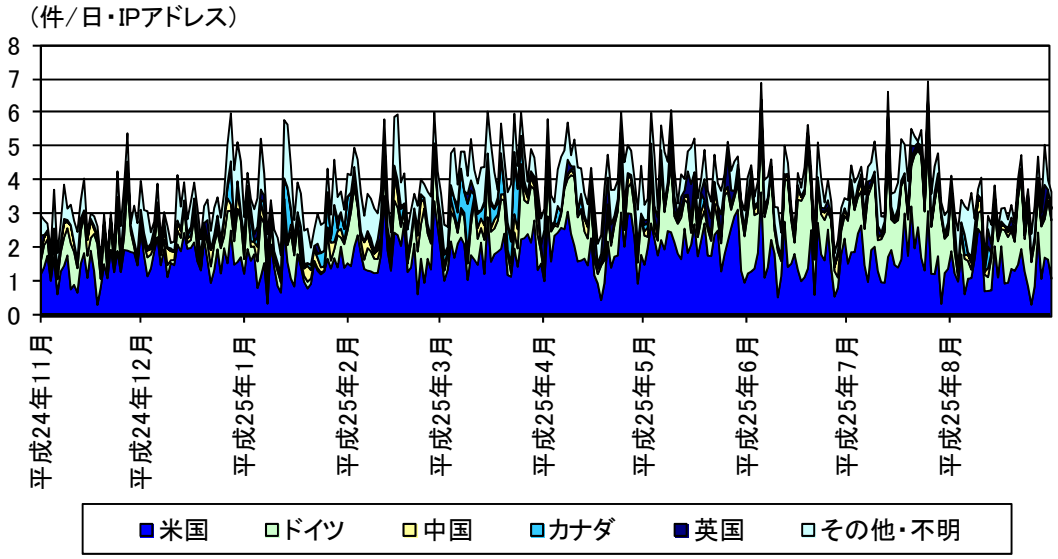

図 2　宛先ポート 5060/UDP に対するアクセス件数の推移（H24.11.1～H25. 8. 31）

検知したアクセスの多くが SIP の「OPTIONS」メソッドであり、このメソッドは SIP サーバなどの VoIP/SIP 機器に対するオプション機能や能力の問合せを行うものです。このことから、同ポートに対するアクセスについては、SIP サーバなどの情報収集を目的とした探索が行われていると考えられます。

なお、観測したアクセスと同様のメソッドを送出するツールが配布されていることを確認しています。このようなツールの機能には、辞書攻撃によりパスワードを探索するものもあり、適切なパスワードが設定されていない場合は、機器の操作権限が奪取される可能性があります。

また、通信事業者等において注意喚起が行われていますが、悪意のある第三者による「なりすまし」や「乗っ取り」によりインターネット経由で国際通話等を利用され、かけた覚えのない国際通話料金が請求されたという事象が発生しており、JPCERT/CC においても SIP サーバを探索するパケットの増加[3]を認知しています。

2　対策について

SIP サーバなどの VoIP/SIP 機器をインターネットに接続している場合は、セキュリティの再確認をお勧めします。考えられるものとして以下のようなものがあります。

- ユーザ ID とパスワードは適切に設定する。
- VoIP/SIP 機器等の設定を確認し、適切なアクセス制限をする。
- VoIP/SIP 機器のソフトウェアにセキュリティ修正プログラムが存在する場合は、最新の状態にしておく。
- 国際通話を利用しない場合は、国際電話の利用休止を通信事業者に相談する。

[3] SIP サーバの不正利用に関する注意喚起（平成 25 年 9 月 6 日）
https://www.jpcert.or.jp/at/2013/at130036.html