平成 28 年3月 10 日

Topic

SIP[i]サーバの探索と考えられるアクセスの増加について

SIP サーバの探索と考えられるアクセスは平成 24 年 11 月以降継続して増加しており、1 か月当たりのアクセス件数は 28 年2月で 24 年 11 月の約 5.9 倍となっています。SIP アカウント(内線番号)に推測可能なパスワードを設定している場合、IP 電話が不正に利用される可能性があるため、セキュリティ対策の再確認を推奨します。

1 SIP サーバの探索

IP 電話機等で使用されている通信プロトコル SIP が利用するポート 5060/UDP に対するアクセスは、平成 24 年 11 月頃から増加しており、25 年9月に注意喚起[ii]を実施しました。その後も継続して増加しており、28 年2月には増加し始めた 24 年 11 月の約 5.9 倍のアクセスを観測しました(図1)。

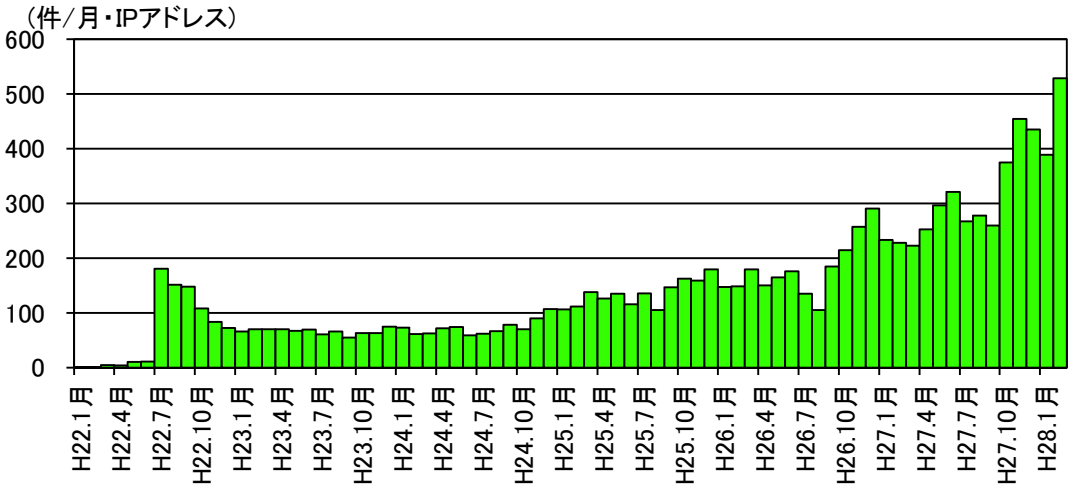

図1 宛先ポート 5060/UDP に対するアクセス件数の推移(1 か月 1IP アドレス当たり)
(平成 22 年1月～28 年2月)

2 探索ツールを使用したアクセス

観測したアクセスは、ほぼ SIP サーバのバージョン、許可されているメソッド、稼働状況等の問い合わせを行う「OPTIONS」メソッドでした(図2)。インターネット上には、「OPTIONS」メソッドを利用して稼動している SIP サーバを探索するためのツール(以下「探索ツール」という。)が公開されており、観測したアクセスの多くは、探索ツールを使用したものと考えられるものでした(図3)。また、探索ツールの他にも SIP サーバに登録されている SIP アカウント(内線番号)を探索するツール、SIP アカウントに設定されたパスワードを辞書攻撃等で探索する

[i] 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)といいます。SIP(Session Initiation Protocol)は、VoIP で使用される通信プロトコルで発信、着信、応答、切断といった制御を行います。

[ii] 「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」(平成 25 年9月6日)
http://www.npa.go.jp/cyberpolice/detect/pdf/20130906.pdf

ツールも公開されていることから、存在が明らかになった SIP サーバに対して SIP アカウント及びパスワードの探索が行われることが考えられ、SIP アカウントに推測可能なパスワードを設定している場合には、IP 電話が不正に利用される可能性があります。

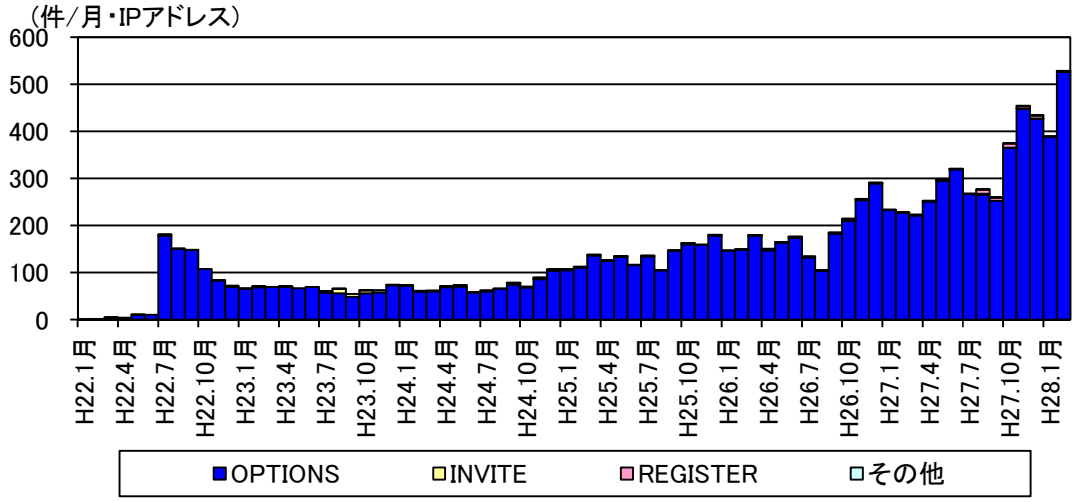

図2　宛先ポート 5060/UDP に対するアクセス件数の推移（メソッド別）
（平成 22 年1月～28 年2月）

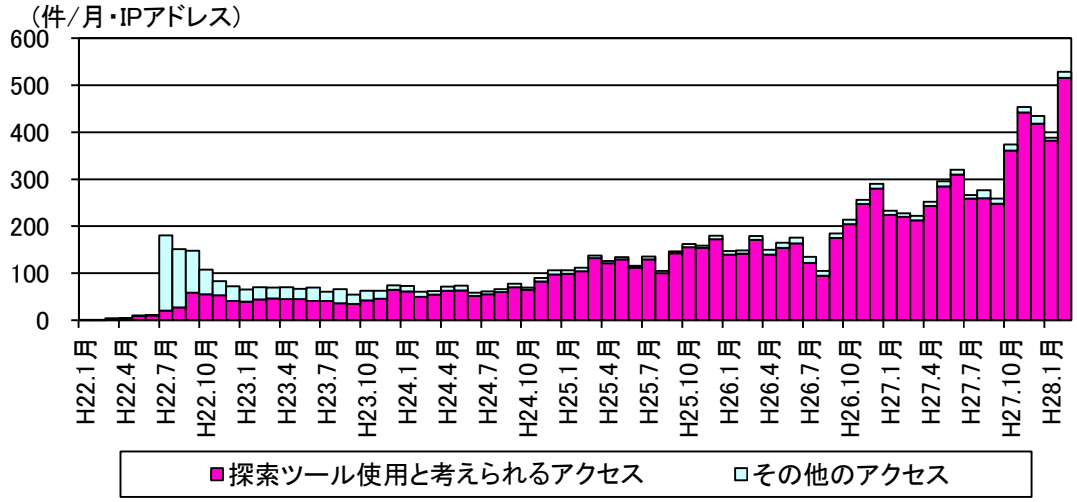

図3　宛先ポート 5060/UDP に対するアクセス件数の推移（探索ツール使用の有無別）
（平成 22 年1月～28 年2月）

探索ツールを使用したと考えられるアクセスに着目すると、5060/UDP 以外のポートでも探索ツールを使用したと考えられるアクセスが観測されました（図4）。多くは、5061/UDP、5070/UDP といった 5060/UDP に近いポートに対するアクセスでした（表）。

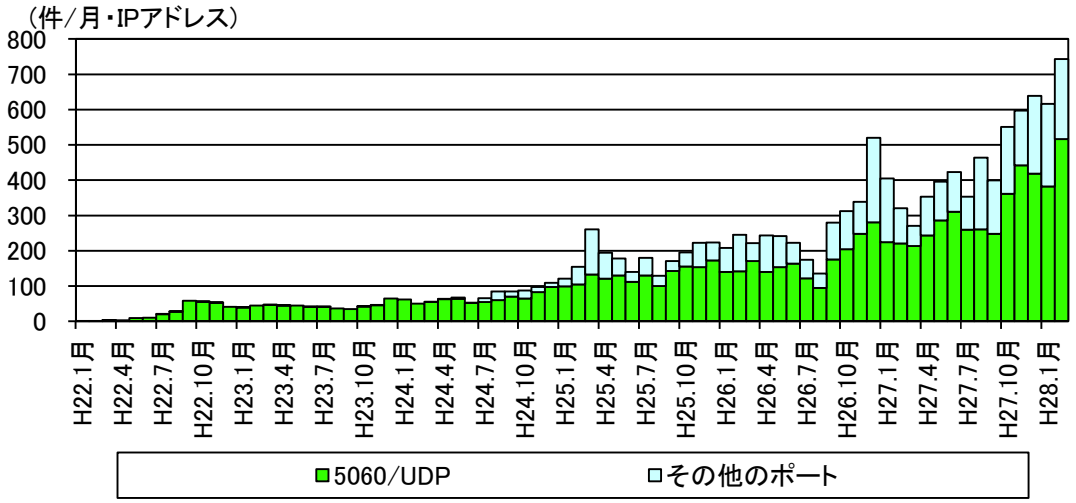

図4　探索ツールを使用したと考えられるアクセス件数の推移（宛先ポート別）
（平成 22 年1月～28 年2月）

表　探索ツールを使用したと考えられるアクセスの主な宛先ポート

ポート	アクセスに占める割合
5060/UDP	71.6%
5061/UDP	1.4%
5070/UDP	1.4%
5080/UDP	1.1%
5065/UDP	0.8%
5090/UDP	0.8%
5064/UDP	0.7%
6060/UDP	0.7%
5069/UDP	0.7%
5063/UDP	0.7%

以上のことから、SIP サーバの探索行為は、幅広いポートに対して行われていることがうかがわれます。このことから、ポートを変えて SIP サーバを運用している場合においても、注意が必要です。

3 対策

SIP サーバや IP 電話を利用する場合は、以下のようなセキュリティ対策が考えられます。

- パスワードを推測されやすいものに設定しない。
- SIP サーバのアクセス制限をし、必要なところからのみアクセスを許可する。
- 使用する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適用する。

SIP サーバや IP 電話の不正利用に関しては、平成 25 年9月に JPCERT/CC[i]から、27 年6月には総務省[ii]から注意喚起が公開されるなど以前から複数の組織による注意喚起が行われています。これらの注意喚起を参考にセキュリティ対策の再確認を推奨します。

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

[ii] 「第三者による IP 電話等の不正利用に関する注意喚起」(総務省:平成 27 年 6 月 12 日)
http://www.soumu.go.jp/menu_kyotsuu/important/kinkyu02_000191.html