

Topic

平成 22 年 6 月 15 日

## 9415/TCP に対するアクセスの増加について

公開プロキシサーバの探索と考えられる特異なアクセスの増加を検知しています。

警察庁では、平成 21 年 11 月頃から、主として中国の不特定の IP アドレスを発信元とした、9415/TCP に対するアクセスの増加を検知しています。このアクセスは、平成 22 年 2 月末頃から、急増しています。(図1)

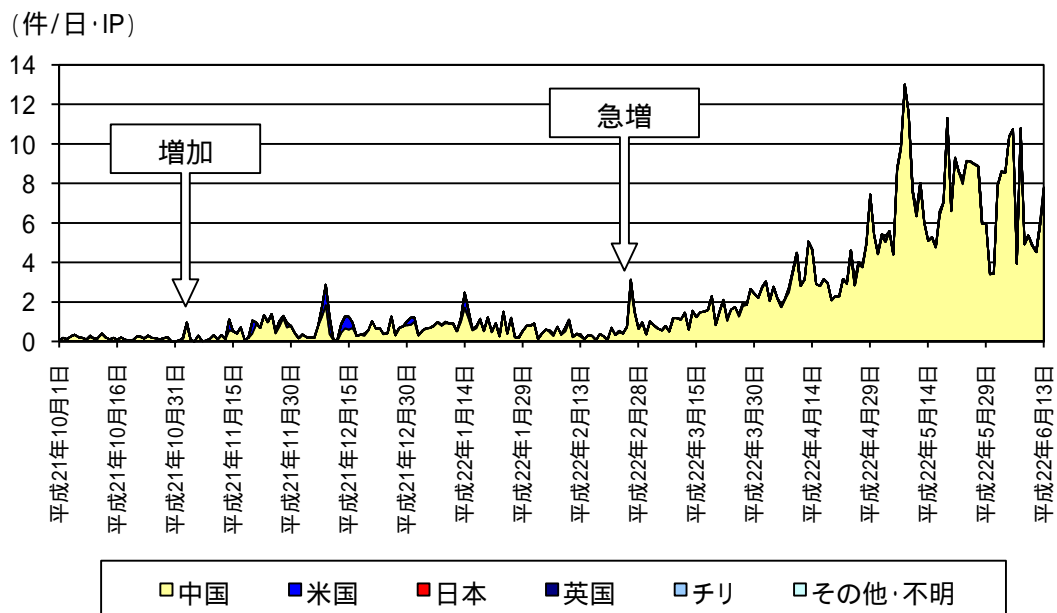


図1 9415/TCP に対するアクセス状況

この 9415/TCP に対するアクセスは、発信元ポートのほとんどが 6000 となっています。発信元ポートの 6000 は、ツールを使用したスキャン<sup>1,2</sup>で使用されてきたポートであり、今回のアクセスも、スキャンツールを使用したアクセスであると考えられます。

さらに、アクセスに対して応答する「SYNACKER センサー<sup>3</sup>」による観測では、スキャンを行った後に、プロキシサーバとして動作するか確認するため、外部サイトへの接続要求を行っていることがわかりました。

<sup>1</sup> 「我が国におけるインターネット治安情勢(平成 21 年 7 月期)」 pp.4-8 「2-2 Oracle 社製データベースソフトへの攻撃ツール」  
(<http://www.cyberpolice.go.jp/detect/pdf/20090831.pdf>)

<sup>2</sup> 「我が国におけるインターネット治安情勢(平成 21 年 10 月期)」 p.8 「3 インターネット定点観測 センサーに対するアクセス」  
(<http://www.cyberpolice.go.jp/detect/pdf/20091214.pdf>)

<sup>3</sup> 「我が国におけるインターネット治安情勢(平成 21 年 7 月期)」 p.5 「(2)SYNACKER センサー」  
(<http://www.cyberpolice.go.jp/detect/pdf/20090831.pdf>)

9415/TCP を外部から利用可能な公開プロキシサーバとして動作させるソフト<sup>1</sup>も存在します。今回のアクセスの目的は、このようなソフト利用者のパソコンをはじめとした、公開プロキシサーバの探索であると考えられます。

使用しているパソコンが、公開プロキシサーバとして動作している場合、外部サイトへの DoS 攻撃<sup>2</sup>や Web サイトの掲示板への悪意のある書き込み<sup>3</sup>を行う際の踏み台として利用されるおそれがあります。

このような踏み台として利用されないように、

**公開プロキシサーバとして動作するソフトを不用意に使用しない。  
プロキシサーバとして動作するソフトを使用する場合は、ソフトの設定での接続制限を行う。  
ルータ、ファイアウォール及びセキュリティ対策ソフトにより、外部からの接続制限を行う。**

等の対策が必要です。

使用しているパソコンを、外部からの接続を許可する設定としている場合や、サーバとして常時動作させている場合には、特に注意が必要です。

---

<sup>1</sup> 中国の動画共有サイト「Tudou (<http://www.tudou.com/>)」の動画ダウンロード補助ソフト「TudouVa」

<sup>2</sup> システム/ネットワーク管理者向け被害事例と対処法「DoS 攻撃を受けて、サーバが利用不能になった」  
(<http://www.cyberpolice.go.jp/case/taisho08.html>)

<sup>3</sup> システム/ネットワーク管理者向け被害事例と対処法「Web サイトの掲示板に、悪意のある書き込みを大量にされた」  
(<http://www.cyberpolice.go.jp/case/taisho17.html>)