平成 28 年3月 10 日

インターネット観測結果等

（平成 28 年2月期）

- 宛先ポート 500/UDP 及び 4500/UDP に対するアクセスが増加
- 脆弱性が存在する統合ネットワーク管理ソフトウェアを探索する目的と考えられるアクセスを観測

1 宛先ポート 500/UDP 及び 4500/UDP に対するアクセスが増加

今期は、2月 10 日以降、500/UDP を宛先ポートとするアクセスの一時的な増加を観測しました（図1）。500/UDP は IPsec で使用される鍵交換認証プロトコルである IKE（Internet Key Exchange）において使用されるポートです。

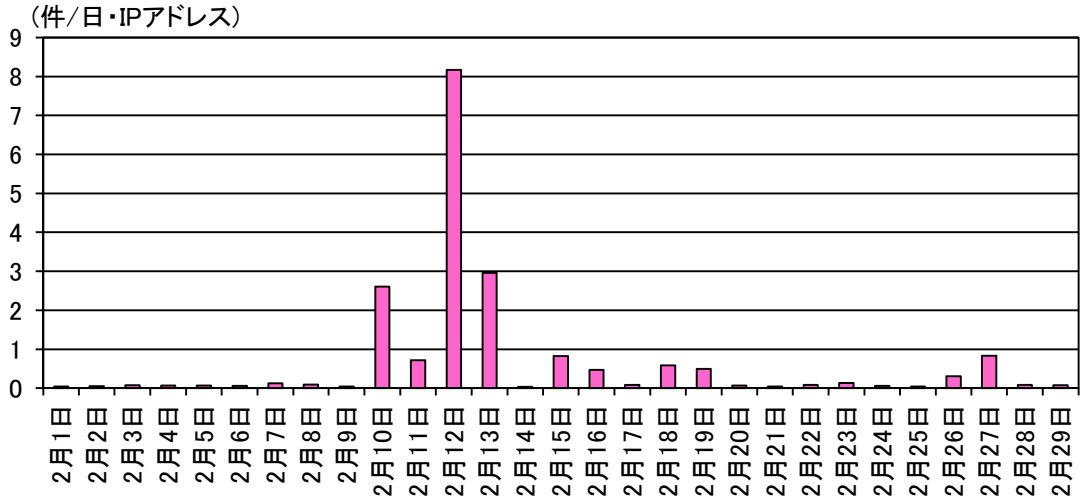

図1 宛先ポート 500/UDP に対するアクセス件数の推移

アクセスが増加した2月 10 日には、Cisco 社から、同社のセキュリティ製品上で動作している Cisco ASA ソフトウェアに重大な脆弱性が存在することが公表[i]されました。当該脆弱性は Cisco ASA ソフトウェアにおける IKE の実装に存在し、当該脆弱性が悪用された場合、攻撃者によって遠隔で任意のコードを実行される可能性があるとされています。また、セキュリティ機関の SANS ISC（Internet Storm Center）は、当該脆弱性を狙った攻撃は宛先ポート 500/UDP 及び 4500/UDP に対して行われる可能性が高く、既に 500/UDP に対するアクセスの増加を観測していることを公表[ii]

[i] 「Cisco ASA Software IKEv1 and IKEv2 Buffer Overflow Vulnerability」
http://www.cisco.com/cisco/web/support/JP/113/1136/1136396_cisco-sa-20160210-asa-ike-j.html
「Cisco Adaptive Security Appliance (ASA) の IKEv1 と IKEv2 の処理にバッファオーバーフローの脆弱性」
http://jvndb.jvn.jp/ja/contents/2016/JVNDB-2016-001382.html

[ii] 「Critical Cisco ASA IKEv1/v2 Vulnerability. Active Scanning Detected」
https://isc.sans.edu/diary/Critical+Cisco+ASA+IKEv2v2+Vulnerability.+Active+Scanning+Detected/20719

しています。

警察庁の定点観測システムにおいても、宛先ポート 500/UDP へのアクセスの増加とほぼ同時期に、宛先ポート 4500/UDP への一時的なアクセスの増加を観測しました（図2）。

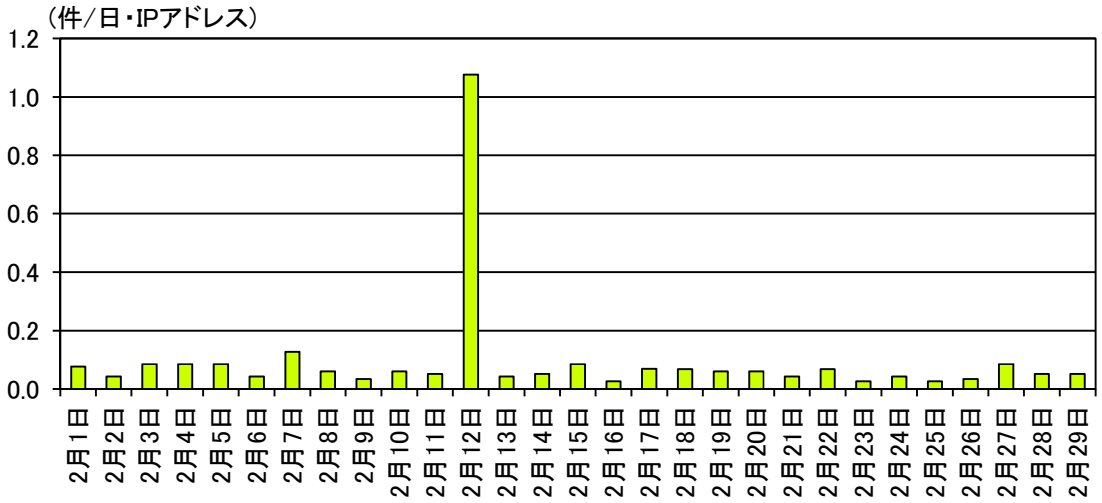

図2　宛先ポート 4500/UDP に対するアクセス件数の推移

宛先ポート 500/UDP 及び 4500/UDP に対するアクセスの増加と当該脆弱性との具体的な関連性は不明ですが、攻撃者が同ポートにアクセスした際の応答状況を調査する等の攻撃の準備行為を行っている可能性も十分考えられます。このため、当該脆弱性の影響を受ける機器の利用者は、ソフトウェアを最新のバージョンにアップデートするなどして、脆弱性を修正することを推奨します。

2　脆弱性が存在する統合ネットワーク管理ソフトウェアを探索する目的と考えられるアクセスを観測

2月3日、Netgear 社が開発販売する統合ネットワーク管理ソフトウェア「NMS300」に存在する脆弱性[i]が明らかとなりました。当該脆弱性は、脆弱性が存在するプログラム（Java サーブレット）に対して細工された HTTP POST リクエストを送信することにより、任意のファイルのアップロードが可能となるものです。当該脆弱性を悪用して Java 言語で記載されたファイル（JSP ファイル）をアップロードし、同ファイルを実行することにより、攻撃者は任意のコードを実行することができます（図3）。インターネット上に、同攻撃手法の具体的な手順が公開されていることも確認しています。

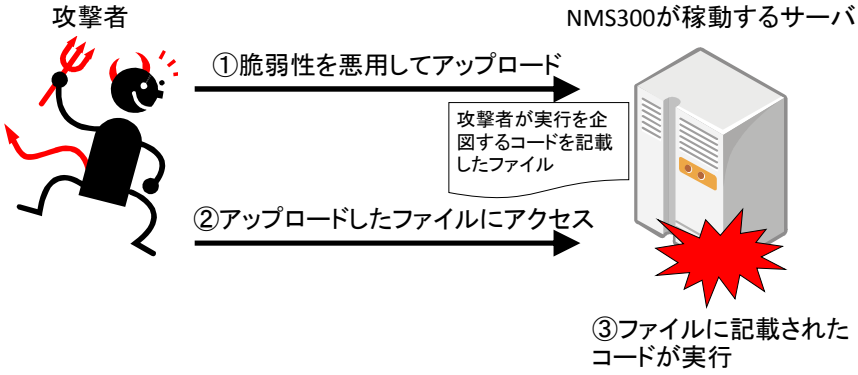

図3　当該脆弱性を悪用する攻撃シナリオ

警察庁の定点観測システムにおいては、当該脆弱性が存在するプログラム（Java サーブレット）に対するアクセスを、2月6日に観測しました（図4及び5）。

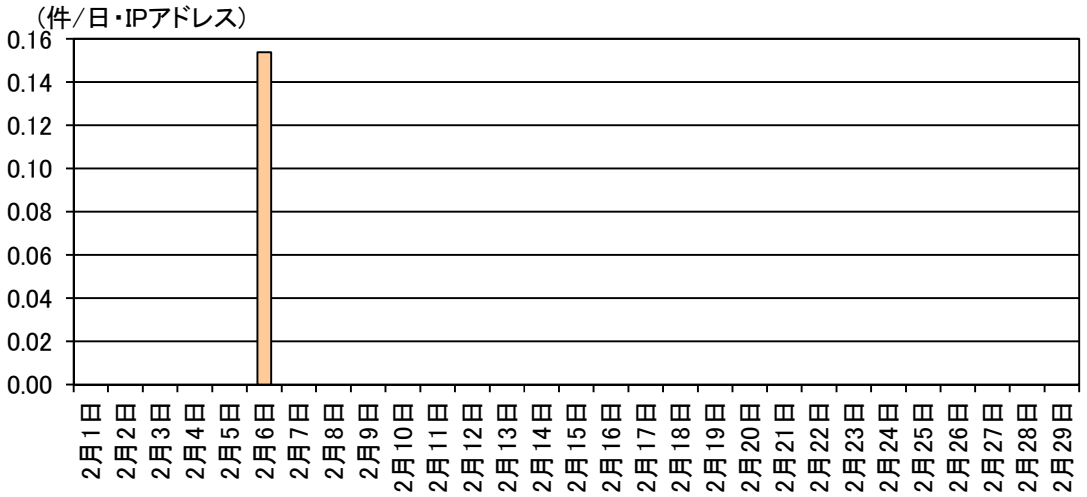

図4　当該脆弱性が存在するプログラム（Java サーブレット）に対するアクセスの観測状況

[i] 「Netgear Management System NMS300 contains arbitrary file upload and path traversal vulnerabilities」
https://www.kb.cert.org/vuls/id/777024
「Netgear NMS300 に任意のファイルアップロードとパストラバーサルの脆弱性」
http://jvn.jp/vu/JVNVU96743693/

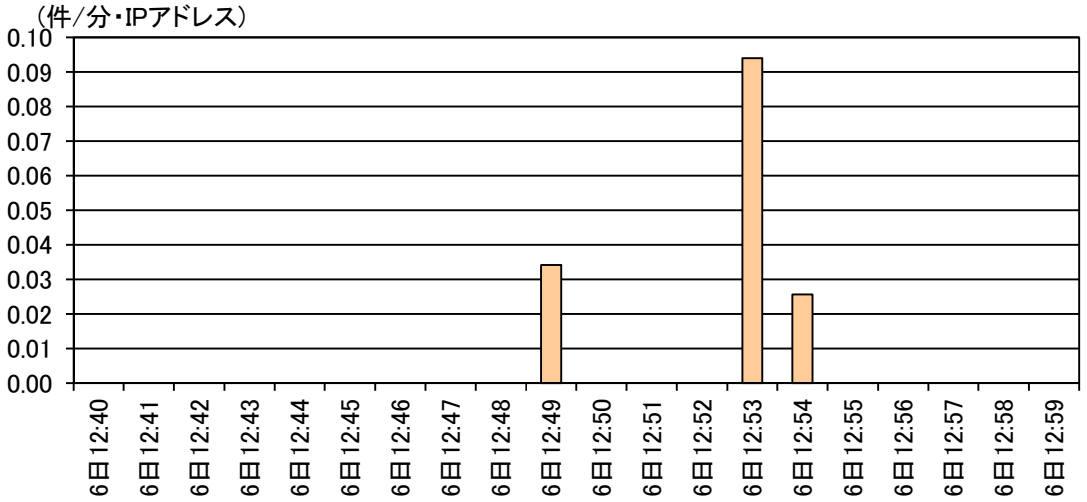

図5　当該脆弱性が存在するプログラム（Java サーブレット）に対するアクセスの観測状況
（2月6日 12:40～13:00）

当該アクセスは、宛先ポート 8080/TCP に対して、脆弱性が存在するプログラム（Java サーブレット）の有無を調査するものであり、直接脆弱性を悪用するものではありませんでした（図6）。しかしながら、同アクセスにより脆弱性が存在することが判明した機器に対しては、さらに脆弱性を悪用する攻撃が行われる可能性が考えられます。

```
GET /fileUpload.do HTTP/1.1
Host: ■.■.■.■
```

図6　観測したアクセスの内容（一部にマスキングを実施）

開発販売元である Netgear 社からは、当該脆弱性を修正したプログラムは公開されていません（平成 28 年3月 10 日現在）。このため、同ソフトウェアを利用している場合にあっては、同ソフトウェアのウェブ管理画面に対するアクセスをファイアーウォール等で適切に制限することを推奨します。具体的には以下に例示する対策等が考えられます。

- 同ソフトウェアのウェブ管理画面は 8080/TCP ポートで動作していることから、ファイアーウォール等で同ポートを宛先とするアクセスを適切に制限する。
- インターネット上からウェブ管理画面にアクセスする必要がない場合は、アクセスを遮断する。
- インターネット上からウェブ管理画面にアクセスする必要がある場合には、信頼できる特定の IP アドレスからのアクセスのみを許可する、又は VPN を経由したアクセスに切り替える等の対策を実施する。