平成 27 年8月 27 日

インターネット観測結果等

（平成 27 年7月期）

- アプリケーションサーバ「GlassFish」で使用されるポートに対するアクセスの増加
- 宛先ポート 500/UDP に対するアクセスが増加
- 産業制御システム用通信プロトコル DNP3 で使用されるポートに対するアクセスの増加

1　アプリケーションサーバ[i]「GlassFish」で使用されるポートに対するアクセスの増加

GlassFish は、オープンソースの Java EE[ii]準拠のアプリケーションサーバです。この GlassFish の管理や設定等を行うための管理コンソールへの接続には、デフォルトで 4848/TCP ポートが使用されます。

定点観測システムにおいては、2月頃からGlassFish の管理コンソールを標的とするアクセスを継続して観測しており、7月にはアクセスの増加を観測しました(図 1)。

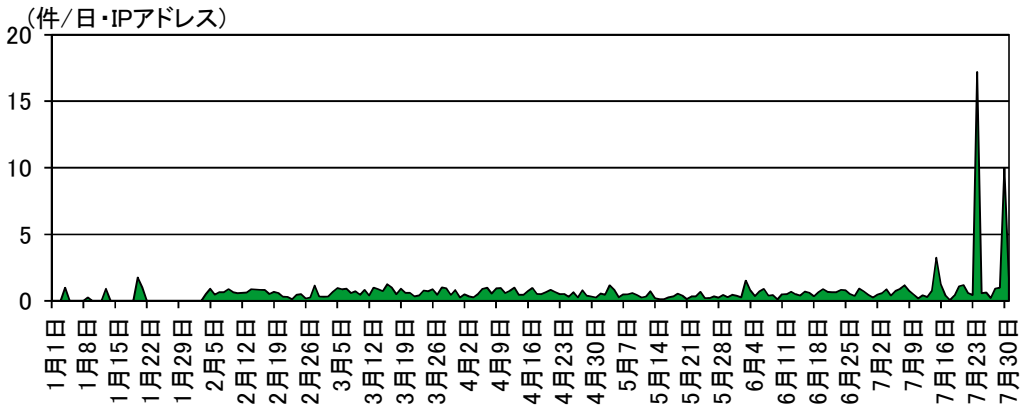

図1　GlassFish の管理コンソールを標的とするアクセス件数の推移（H27.1.1～7.31）

増加したアクセスを分析したところ、GlassFish の管理コンソールにログインを試みるパケットが多数存在しました。このログインを試みるアクセスの発信元については、アクセスを行っている者の実体や目的について判明しておらず、悪用する目的で探索活動を行っている可能性も考えられます。

---

[i] アプリケーションサーバとは、ユーザからの要求を受け付けてプログラムの実行環境やデータベースへの接続機能等を提供しアプリケーションを実行するサーバソフトウェア。

[ii] Java EE は、プログラミング言語の Java によるサーバアプリケーション開発等のための標準仕様。

管理コンソールに不正にアクセスされるとデータの窃取や改ざん等を行われる危険性があるため、管理者においては以下の対策を実施することを推奨します。

- ログインに必要なパスワードを初期の設定から変更する。また、パスワードは、十分な強度があり、容易に推測できないものにする。
- 不特定の IP アドレスからは接続できないように、適切なアクセス制限を実施する。
- 使用している製品について最新のセキュリティ情報を確認し、必要に応じてソフトウェアのアップデートを実施する。

2 宛先ポート 500/UDP に対するアクセスが増加

定点観測システムにおいては、7月8日、23 日及び 24 日に 500/UDP を宛先ポートとするアクセスの増加を観測しています（図2）。

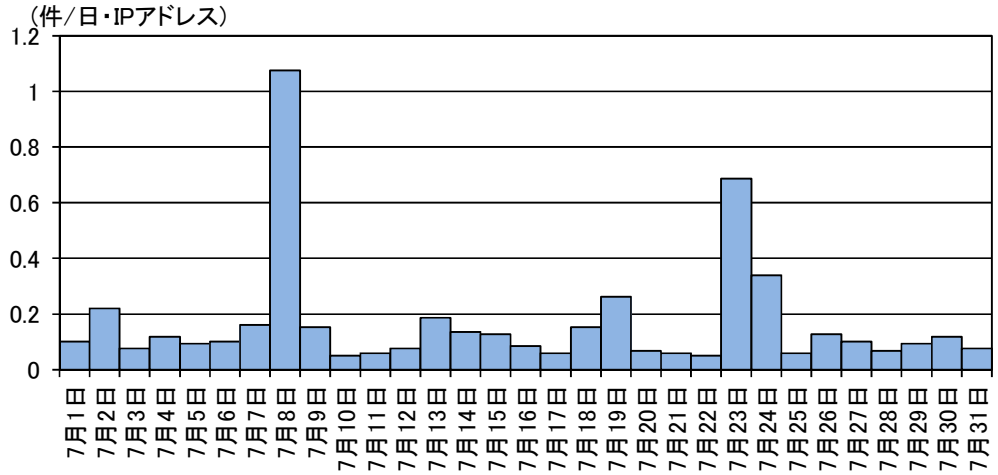

図2 宛先ポート 500/UDP に対するアクセス件数の推移

7月9日に Cisco 社製「セキュリティ アプライアンス ソフトウェア」の脆弱性に関する攻撃を確認したとの情報[i]が公表されました。この脆弱性[ii]は、IPsec で使用される鍵交換認証プロトコルである IKE の実装に存在し、IKE では 500/UDP のポートが使用されます。

この脆弱性を悪用した攻撃を受けると、攻撃の対象となったソフトウェアがサービス不能に陥るなどの可能性があるため、影響するバージョンのソフトウェアを使用している利用者は脆弱性が修正された最新バージョンに更新することを推奨します。

---

[i] 「Multiple Vulnerabilities in Cisco ASA Software」
http://www.cisco.com/cisco/web/support/JP/112/1126/1126286_cisco-sa-20141008-asa-j.html
「Cisco 社製セキュリティアプライアンスソフトウェアの 脆弱性に関する注意喚起」
https://www.jpcert.or.jp/at/2015/at150021.html

[ii] 「Cisco ASA ソフトウェアの VPN コンポーネントの IKE の実装におけるサービス運用妨害（DoS）の脆弱性」
http://jvndb.jvn.jp/ja/contents/2014/JVNDB-2014-004657.html

３　産業制御システム用通信プロトコル DNP3 で使用されるポートに対するアクセスの増加

DNP3 は産業制御システム用の通信プロトコルであり、米国、オーストラリア等において電力や水道のシステムで多く利用され、遠方にあるコンピュータと制御・監視を行うコンピュータとの間の通信等において、データ情報、制御コマンド等の送受信を行うものです。

定点観測システムにおいては、DNP3 で使用される 20000/TCP を宛先ポートとするアクセスの増加を定期的に観測しており、7月下旬にもアクセスの増加を観測しました（図3）。

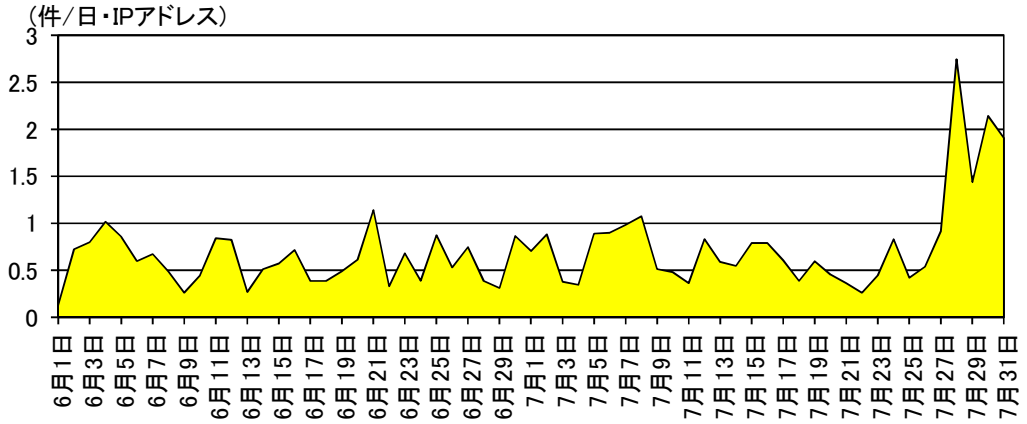

図3　宛先ポート 20000/TCP に対するアクセス件数の推移

DNP3 で接続された機器を探索するためのツールがインターネット上に公開されており、観測したパケットの中には、ツールの特徴を示す情報が含まれるものが多数存在しました。DNP3 を利用して稼動する機器の探索が広く行われている可能性が考えられます。