平成 26 年 7 月 22 日

インターネット観測結果等

(平成 26 年 6 月期)

- **サーバコントロールパネルの探索と考えられるアクセスが急増**
- **サーバ管理チップの脆弱性を狙ったアクセスが増加**

1 サーバコントロールパネルの探索と考えられるアクセスが急増

今期は、宛先ポート 7778/TCP に対するアクセスが急増しました。アクセスは 9 日以降に増加し、今期末までアクセスが継続しています（図 1）。

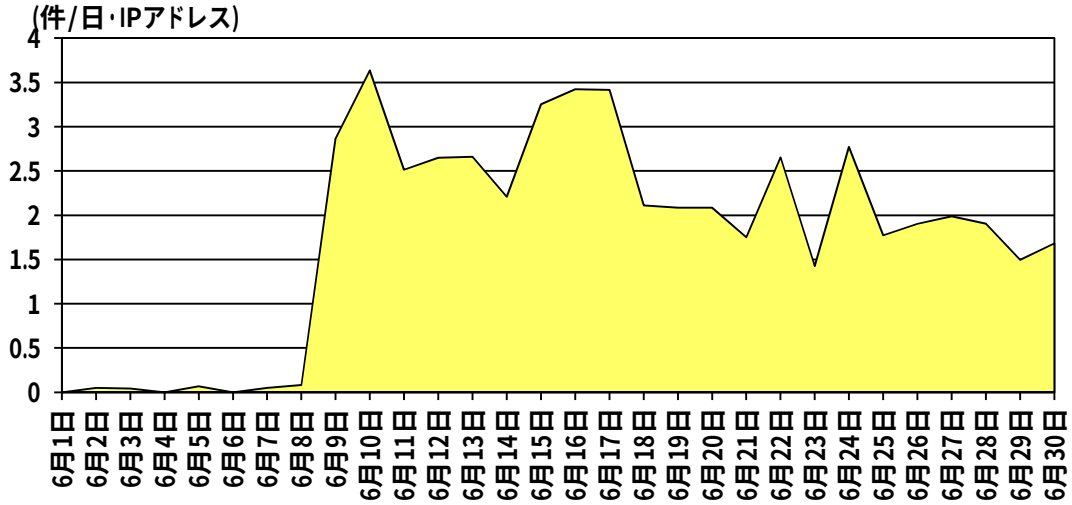

図 1　宛先ポート 7778/TCP に対するアクセス件数の推移

これらのアクセスの多くは、HTTP リクエスト「HEAD / HTTP/1.0」を送信するものでした。このことから、同アクセスは 7778/TCP でウェブサーバが稼動している IP アドレスを探索する目的であると考えられます。

サーバの管理においては、ウェブ画面上からサーバの管理や操作が容易に実施できる「コントロールパネル」と呼ばれるサーバ管理ソフトウェアが使用される場合があります。7778/TCP は、コントロールパネルの管理画面でも使用されるポートです。また、これらのアクセスの発信元 IP アドレスについて調査した結果、幾つかの発信元 IP アドレスの 7778/TCP ポートにおいて、同コントロールパネルのログイン画面が表示されることが確認できました。

このことから、宛先ポート 7778/TCP に対するアクセスは同コントロールパネルがインストールされており、外部から管理画面へアクセスが可能なサーバの探索を実施している可能性が考えられます。また、ログイン画面が表示される発信元 IP アドレスについては、既に同コントロールパネル経由で侵入されており、新たな探索活動の踏み台となっている可能性も考えられます。

他のコントロールパネルにおいても、管理が不十分なまま放置された場合には、サーバへ不正に侵入される危険性があります。コントロールパネルを利用する組織等においては、以下の点に留意することを推奨します。

- 使用しているコントロールパネルのバージョンを最新の状態に保ち続ける。
- コントロールパネルのログインに必要なID・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とする。また他のサービスで使用しているアカウントのID・パスワードを使いまわさないようにする。
- コントロールパネルの画面は、不特定な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。

2 サーバ管理チップの脆弱性を狙ったアクセスが増加

サーバ用途に設計されたコンピュータ用マザーボードには、BMC（Base Management Controller）と呼ばれるサーバ管理チップが搭載されることがあります。BMC によって提供されるサーバ管理機能は、製造メーカごとに異なった名称が付けられており、提供される管理機能にも違いがあります。しかしながら、多くの場合には、BMC に専用のネットワークインターフェースが用意されるとともに、OS や電源投入の状況に左右されずに BMC が常時稼動し続けます。この BMC によりネットワーク経由によるサーバの状態監視、電源操作、キーボード・マウス操作及び画面表示などが可能となります。

6月 19 日、特定メーカが製造するマザーボードに搭載された BMC に脆弱性が存在し、ネットワーク経由で管理者パスワードが取得可能であるとの情報が公表されました。同情報では、管理者パスワードが BMC 内に暗号化されずに保存されており、49152/TCP ポートに特定のリクエストを送信するだけで同パスワードが閲覧可能であるとされています。また、インターネット上を探索した結果、同脆弱性が存在するコンピュータを約 32,000 台確認できたとも報告されています。

定点観測システムにおいても、20 日から宛先ポート 49152/TCP に対するアクセスが観測されています（図2）。これらのアクセスの中には、同ポートの開放状況を確認するアクセスに加えて、同脆弱性を狙ったリクエストを送信するアクセスも多数観測されています。

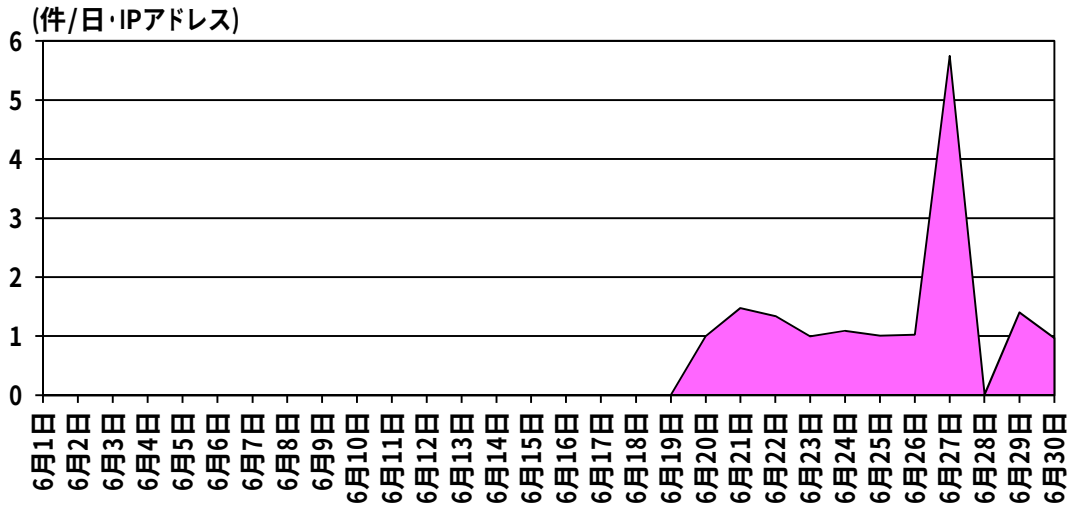

図2　宛先ポート 49152/TCP に対するアクセス件数の推移

BMC については、ハードウェアの一部と見なされ、セキュリティ対策が十分に実施されていない可能性が危惧されます。しかしながら、BMC では OS から独立したプログラムが動作しており、ネットワークにも直接接続されているため、サイバー攻撃の糸口となる可能性を考慮する必要があります。BMC についても、前項のコントロールパネルと同様の対策を実施する必要性があります。