4-1 サイバー攻撃の現状

サイバー攻撃、リアルタイム

世間では、サイバー攻撃が増えている、気をつけたほうがよい、とは聞いていても実際にどの程度のサイバー攻撃が行われているか、リアルタイムで把握するのは難しいと思います。

本節では、攻撃者がどの地域からどの地域に攻撃しているかを見ていきます。

図4-1-1は、「Digital Attack Map」サイトです。このサイトでは、どの程度の攻撃が、どの地域からどの地域へ行われているかを、リアルタイムで確認できます。また、サイトの下側には、タイムラインで過去の攻撃状況も確認できます。また、気になる地域をズーム（拡大）して表示できます。

○図4-1-1：Digital Attacker Map（http://www.digitalattackmap.com/）

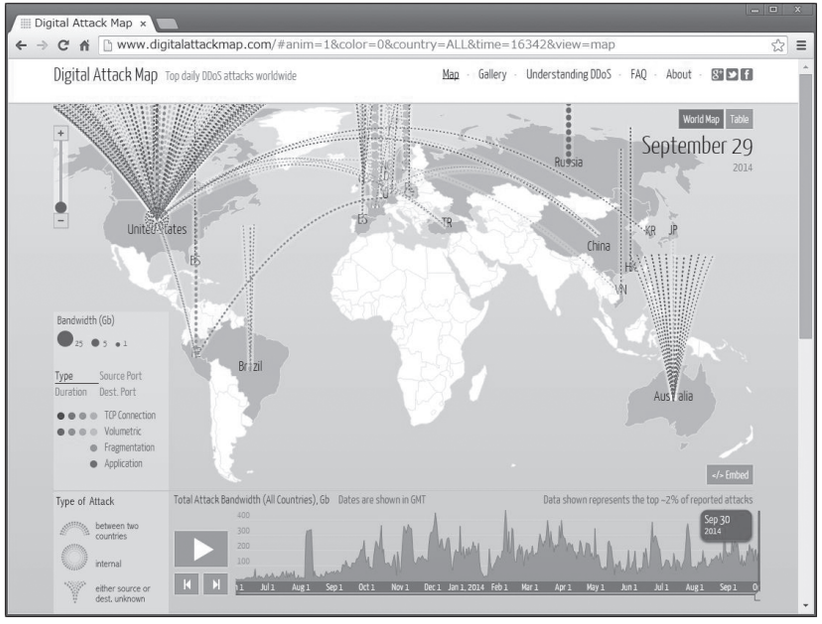


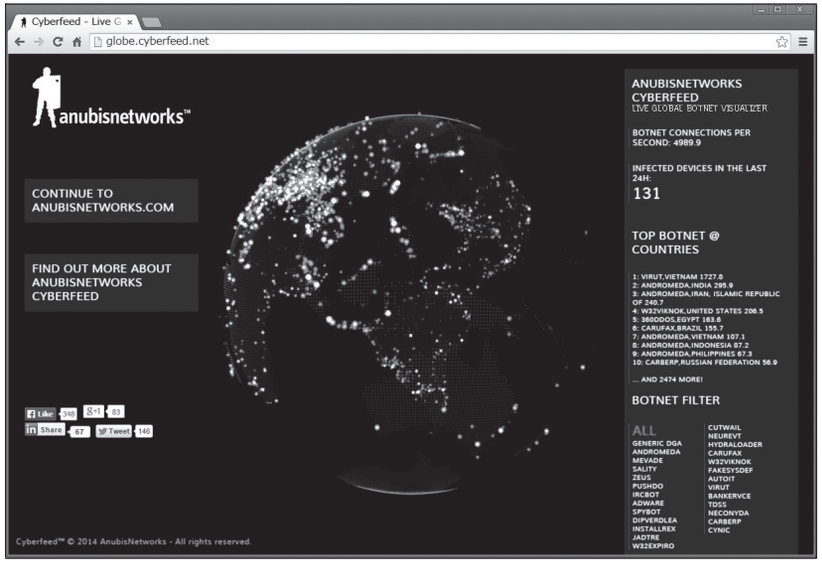
図4-1-2では、ボットネットに感染した地域とボットネット種別が表示されています。リアルタイムで表示されるこの画面から、現状のボットネットの流行とその感染地域を確認できます。

図4-1-3では、攻撃を受けている地域が色づけされています。米国、欧州で攻撃されていることがわかります。また、サイトの下側には、日本付近を拡大しています。

図4-1-4に、「流星」のように見えているものが無数にありますが、これは攻撃の1つで、リアルタイムにどこからどこに攻撃されているかを確認できます。画面左上には、攻撃者地域の順位、画面右上には攻撃を受けている地域の順位が表示されています。また、画面右下には、攻撃の標的となっている上位サービスが表示されているので、どのサービスに対して防御したほうがよいかとの指針になります。加えて、画面下側には、攻撃の詳細がタイムラインで表示されています。

図4-1-5に、「流星」のように見えているものが無数にありますが、これは攻撃の1つで、リアルタイムにどこからどこに攻撃されているかを

○図4-1-2：Cyberfeed（http://globe.cyberfeed.net/）



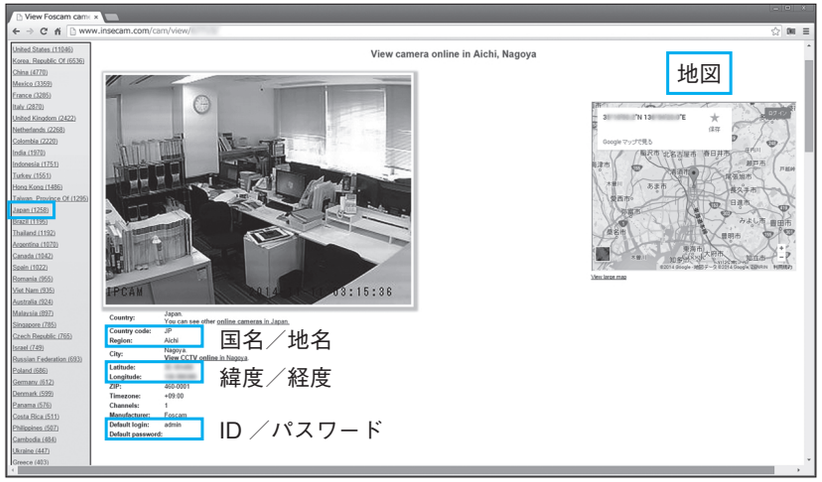
5-11 監視カメラに脆弱なパスワード設定

監視カメラ、Webカメラ、パスワード

インターネット環境の改善に伴い、監視カメラとして、Webカメラが利用される傾向にあります。しかし、デフォルトのパスワードや推測可能な脆弱パスワードで、利用しているケースも見受けられます。セキュリティ研究者の報告によると、256ヶ国に約7万3,000台も存在すると指摘されています。

図5-11-1のように、インターネット上に公開された監視カメラ（Webカメラ）に安易なユーザ名やパスワードが設定されていると、カメラ画像のほかに、国名、地名、緯度/経度、ID/パスワードも漏洩します（この例では、パスワードは設定されていないようです）。緯度/経度が判明するため、おおよその撮影場所までも地図で暴かれてしまいます。

○図5-11-1：Online IP netsurveillance cameras of the world
（http://www.insecam.com/）



対策

監視カメラ（Webカメラ）からカメラ画像他、各種情報が漏洩しないよう、次の対策を検討してください。

- 監視カメラへのアクセス制御（IPアドレスなど）をする
- 推測が困難なIDと複雑なパスワードに変更する

5-12 USBの脆弱性（BadUSB）

USB、BadUSB、ファームウェア、コントローラIC

2014年8月、セキュリティイベント「BlackHat USA 2014」で、USBの脆弱性をデモされました。このデモは、USB挿入時に悪意あるペイロード（Payload）が実行されることを実証したものでした（「BadUSB」と呼ばれています）。当時、その脆弱性を実証するコードは公開されませんでしたが、同年10月に、ソフトウェアコード共有サイト「GitHub」に公開されました。

本節では、このUSB脆弱性の影響とその対策を見ていきます。

USBには、セキュリティ機能が存在しないため、悪意あるペイロードを仕込まれたUSBデバイスを挿入すると、任意のコードなどを実行される可能性があります（**図5-12-1**）。

実際に、USBデバイスのファームウェアを書き換えて、BadUSBを作成してみました。そのBadUSBデバイスを挿入した場合の例を見ていきます。この例では、メモ帳（notepad.exe）を起動し、「Hellow World」を表示しています（**図5-12-2**）。BadUSBデバイスを挿入するだけで、自動で、悪意あるペイロードが実行されます。

悪意あるペイロードは、どのように指定しているのでしょうか。**図5-12-3**は、メモ帳を起動して「Hello World!!!」を表示するものです。このペイロードを悪用すれば、有害なプログラムを起動したり、マルウェア感染したり、端末を乗っ取るなどすることが容易に想像できます。