



■ ホームページ攻撃状況(2016/2/19 付)

571 => 34, 378 IP

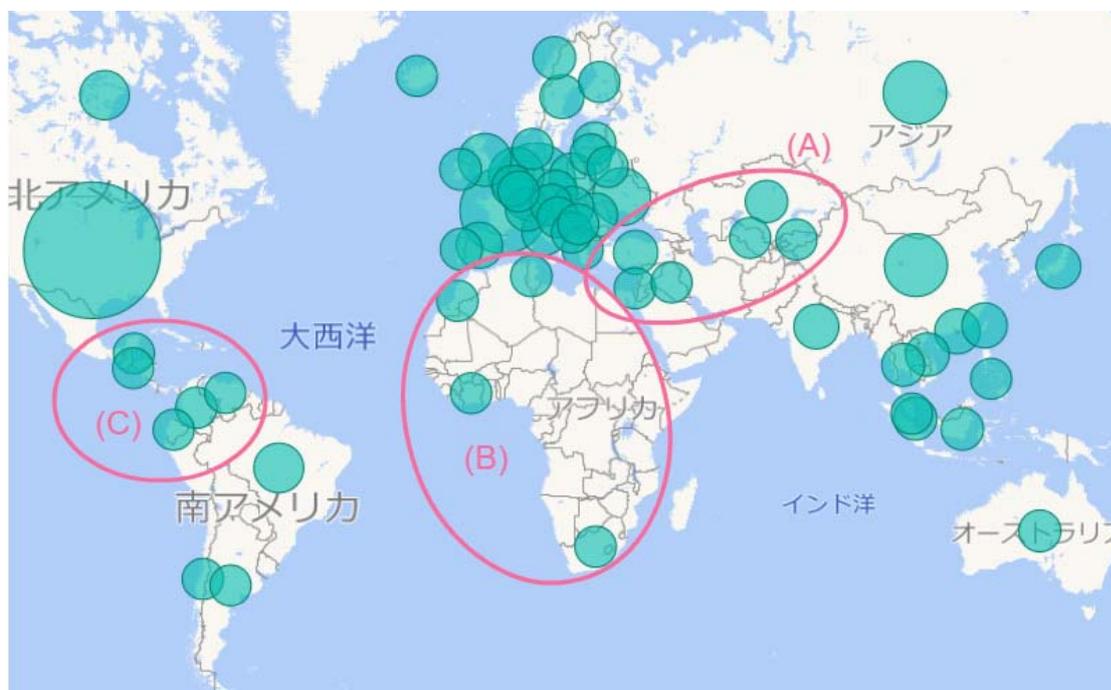
昨年のかわら版7月号で「ウェブサーバーのブラックリスト数」についてお知らせしました。ウェブサーバーのブラックリストとは弊社の運営するウェブサーバー(2017/3/1 現在 9 台)に対して、攻撃を行ったり、不信なアクセスをしたサーバーのアドレスです。このような攻撃はソフトウェアで随時監視していて、ブラックリストに登録されたIPからは弊社の管理するウェブサイトへはアクセスができません。

昨年7月の段階では、攻撃の経歴をソフトウェアで捕捉し、目視によりブラックリストへの登録をしていたのですが、攻撃の頻度(と量)が急激に上昇したため、攻撃パターンに応じてブラックリストへ自動登録するようにシステムを変更しました。

このなかで、特殊ケースとして、小規模なネットワーク(クラスCと言われるネットワーク)内の複数のアドレスから攻撃を受けていることがわかりましたので、ネットワーク単位でのブラックリスト登録も行うことにしました。

この結果、昨年7月に571だけだったブラックリストが、34、378IP(2月17日付)に膨れ上がりました。

下図は最新の攻撃元マップです。アメリカ、ドイツ、フランス、ロシア、中国といった上位国に変化はありませんが、あらたに、中央アジア(A)、アフリカ(B)、中米(C)からの攻撃が発生していることがわかります。



図： 攻撃元マップ

(A)に含まれる6か国は、カザフスタン、キルギスタン、ウズベキスタン、トルコ、イスラエル、イラクです。(B)はチュニジア、モロッコ、コートジボワール、南アフリカ。(C)はエルサルバドル、ベリーズ、エクアドル、コロンビア、ベネズエラとなっています。