平成 26 年 2 月 13 日

インターネット観測結果等
(平成 25 年 12 月期)

● PHP-CGI の脆弱性を狙った攻撃が急増

PHP-CGI に関する脆弱性[1]に関して、平成 25 年 10 月 29 日に新たな攻撃コードが公開されました。同攻撃コードの公開により、PHP-CGI を実際には使用していなくても、PHP-CGI が使用できる状態となっているだけで、脆弱性を利用した攻撃を受ける可能性があることが明らかとなりました。警察庁においては、前期末から今期にかけて、同脆弱性を狙った攻撃の急増を観測しています（図1）。

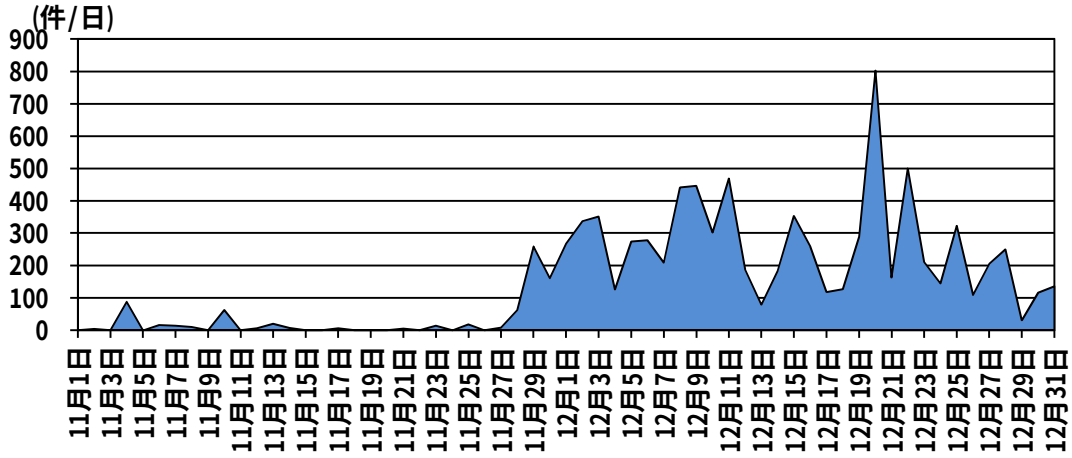

図1　PHP-CGI の脆弱性を狙った攻撃件数の推移（H25.11.1～12.31）

これらの攻撃について分析した結果、ボットプログラムに感染して外部からの攻撃命令を受信し、DoS 攻撃等の攻撃行為の踏み台となる場合もあることが判明しています。同攻撃手法による被害を防止するために、次の対策を推奨します。

- 各組織で管理するウェブサーバで PHP の導入有無と、導入されていた場合には、その PHP のバージョンを確認する。
- PHP のバージョンが以下に該当する場合には、速やかに最新版へのバージョンアップを実施する。
  - PHP 5.3.12 より前のバージョン
  - PHP 5.4.2 より前の PHP 5.4.x
- ウェブサーバの公開ディレクトリ内に、使用していない PHP の実行ファイルもしくはそのシンボリックリンクが存在しないかを確認する。不要なものが存在した場合には、削除を行う。
- 脆弱性が存在するバージョンの PHP が動作していたウェブサーバについては、既に攻撃を受けている可能性があるので、アクセスログの精査を実施すると共に、ファイル作成、プロセス起動及び外部との通信状況について調査を実施する。

[1]「JVNVU#520827 PHP-CGI の query string の処理に脆弱性」（CVE-2012-1823）
http://jvn.jp/cert/JVNVU520827/