平成 27 年5月 26 日

インターネット観測結果等

（平成 27 年4月期）

- SSL/TLS における輸出用グレード暗号に係る脆弱性の探索を目的としたアクセスの観測
- 発信元ポート 53/UDP からのアクセスが一時的に増加

1 SSL/TLS における輸出用グレード暗号に係る脆弱性の探索を目的としたアクセスの観測

平成 27 年3月３日、SSL/TLS における輸出用グレード暗号に係る脆弱性[i]（以下「FREAK」という。）が公表されました。

FREAK は、中間者攻撃によってSSL/TLS 通信の暗号で使われる暗号を、解読可能な暗号強度の弱い輸出用グレード暗号に強制的に設定されるものになります（図1）。これにより通信内容の盗聴や改ざんを行われる可能性があります。

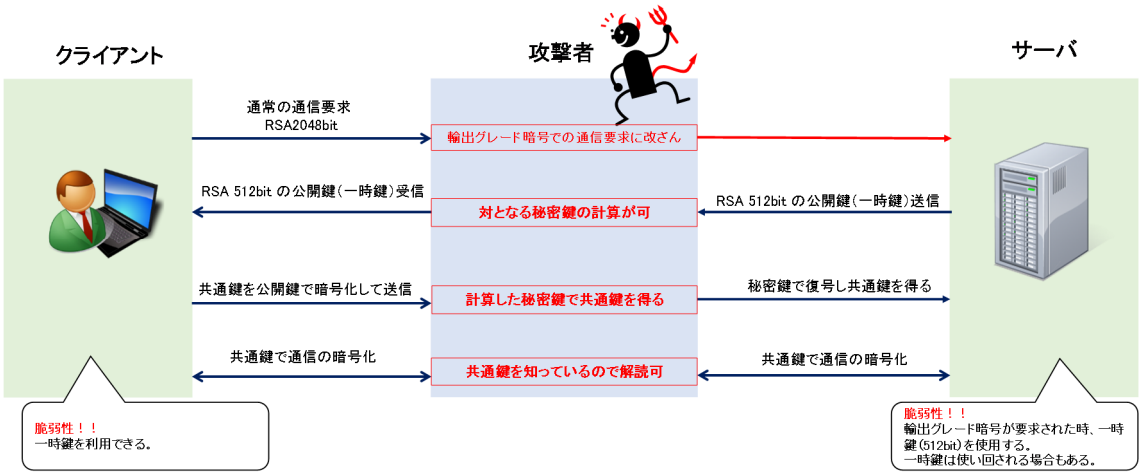

図 1　脆弱性による攻撃手法の概要

警察庁では、FREAK が公表されて以降、海外の調査研究機関が研究目的で当該脆弱性があるサーバを調査していると思われるアクセスを観測しています（図2）。

[i] 「SSL/TLS の実装が輸出グレードの RSA 鍵を受け入れる問題（FREAK 攻撃）」
http://jvn.jp/vu/JVNVU99125992/

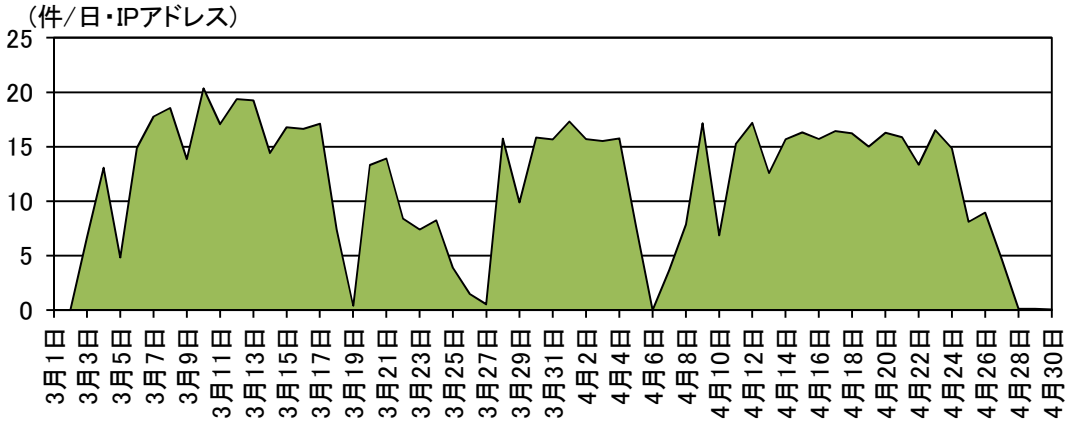

図2　輸出用グレード暗号脆弱性サーバの探索を目的としたアクセス件数の推移
（H27.3.1～4.30）

FREAK は、サーバとクライアントの両方に脆弱性がある場合に成立するものです。それぞれで推奨される対策は以下のとおりです。

サーバ側

- 輸出用グレード暗号のサポートを無効にする

クライアント側

- ウェブブラウザの修正ファイルを適用し最新の状態しておく

2　発信元ポート 53/UDP からのアクセスが一時的に増加

警察庁の定点観測システムでは、4月上旬に発信元ポート 53/UDP からのアクセスの一時的な増加を観測しました（図3）。特に、4月８日に増加しており、その特徴として増加した問い合わせ先ホストは海外のポータルサイトと検索サイトであることが確認しました。該当サイトに対して何らかの攻撃が行われた可能性が考えられます。

4月中全体の発信元ポート 53/UDP からのアクセスを確認すると、多くのパケットは DNS の問い合わせに対する回答であり、発信元 IP アドレスの多くはオープンリゾルバとして動作することを確認しました。そのため、このアクセスは、オープンリゾルバを悪用した DDoS 攻撃によるものであると考えられます。この DDoS 攻撃についての詳細は警察庁の@police の注意喚起[i]を参照として下さい。

[i] 「日本国内のオープン・リゾルバを踏み台とした DDoS 攻撃発生に起因とするパケットの増加について」（平成 26 年7月 23 日）
https://www.npa.go.jp/cyberpolice/detect/pdf/20140723.pdf

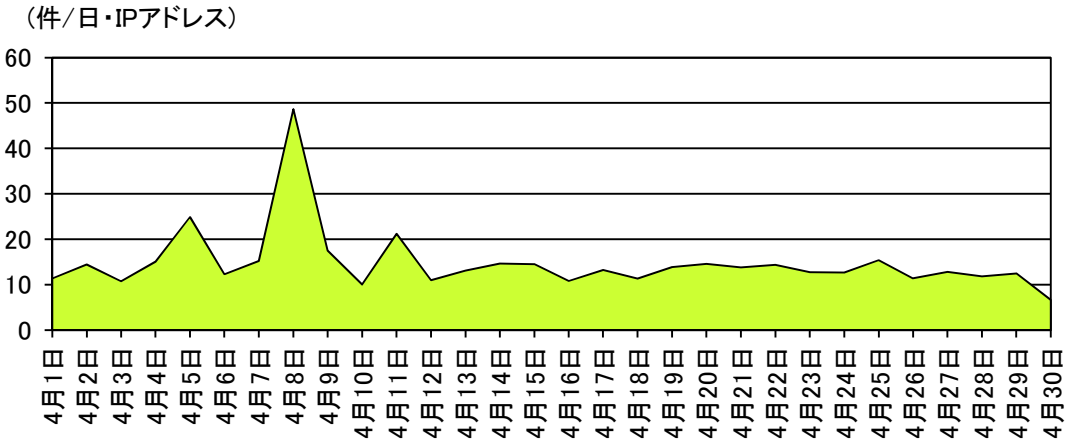

図3　発信元ポート 53/UDP からのアクセス件数の推移