平成 25 年 5 月 16 日

関係者各位

総合情報システム部

DNS アンプ攻撃等に対する対策（オープンリゾルバ対策）について

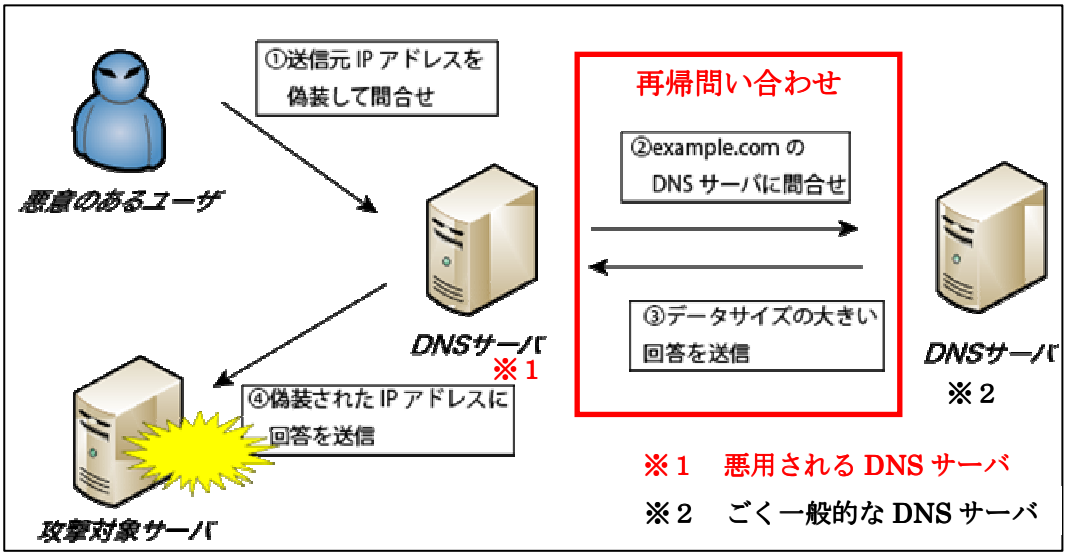
大阪府サイバーテロ対策連絡協議会事務局から以下の告知がありました。

（「別紙１　Spamhaus Project に対する DDoS 攻撃について.pdf」参照）

上記資料によりますと、2013 年 3 月にオープンリゾルバ状態の DNS サーバを悪用した大規模 DDoS 攻撃が欧州で発生しました。本学内においても、DNS サーバが DNS アンプ攻撃・DNS ポイズニング攻撃に悪用される危険性があるため、早急にオープンリゾルバ対策をとる必要がございます。

下記に DNS アンプ攻撃、DNS ポイズニング攻撃の【特徴】と【オープンリゾルバ状態確認方法】と【オープンリゾルバ対策案】を記載いたしますので、必要に応じて対策をお願いします。

【 特徴 】DNS アンプ攻撃とは、DNS の再帰問い合わせ機能を悪用した攻撃です。簡略化した図式は以下になります。



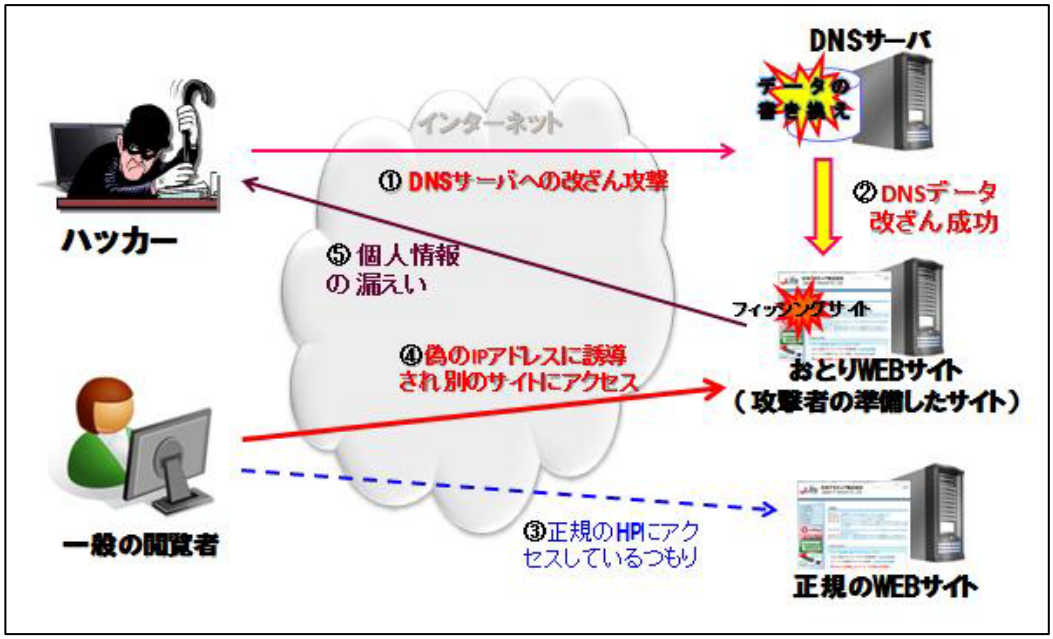
（③は、②に返答データが加算されるのでデータが大きくなります。）

想定される危険性は、以下の２つがあります。

その 1、「攻撃対象サーバ」として近畿大学管理のサーバが攻撃される。

その 2、「悪用される DNS サーバ」として、「大学管理の DNS サーバ」が気づかぬ内に DNS アンプ攻撃に参加してしまう。

DNS ポイズニング攻撃とは、DNS サーバのキャッシュ機能を利用して、悪意あるサイトへ誘導する攻撃方法です。簡略化した図式は以下になります。



想定される危険性は、以下になります。

・「大学管理の DNS サーバ」が改ざん攻撃をうけ「おとり Web サイト」へ一般の閲覧者を誘導してしまう。

以上のように、多様な危険性があるので早急に対策を取る必要がございます。

【オープンリゾルバ状態の確認方法】

管理している DNS サーバが「オープンリゾルバ」（※１）状態かどうかをチェックしてください。

（※1　　不特定からの問い合わせ通信に応答する設定のこと。）

＜確認方法：サーバの設定を確認する＞

DNS サーバが「オープンリゾルバ」状態の場合の設定は以下になります。

・BIND をご利用の場合　ファイル：named.conf

```
allow-query-cache { any; };
allow-recursion { any; };
```

【 オープンリゾルバ対策案 】

≪案１≫

DNS サーバが受ける学外からのキャッシュ参照、及び再帰的な問い合わせを 163.51.0.0 に制限する設定にする。

＜設定内容＞

・BIND をご利用の場合　ファイル：named.conf

```
allow-query-cache { localhost; 163.51.0.0/16; };
allow-recursion { localhost; 163.51.0.0/16; };
```

※　上記設定を行うと、DNS サーバは以下のような動作になります。

「kindai.ac.jp に関する名前問合せ」に対しては今までどおり名前問合せの回答を行います。

「学外のサーバに関する名前問合せ」（例：www.yahoo.co.jp 等）の回答は、再帰問合せに当たるため、回答を行わなくなります。

≪案２≫

「***.kindai.ac.jp」ドメインの名前問合せを、大学が管理している「外部用 DNS サーバ」と「内部用 DNS サーバ」に移管します。そして、現在、管理している DNS サーバの DNS 機能を停止できるようにします。

＜移管計画案＞

①「管理している DNS サーバ」のゾーン情報をすべて「外部 DNS サーバ」に移管します。

②「管理している DNS サーバ」の名前問合せの通信を FW にて遮断します。

――――――　平行運用期間　――――――――――――――――――――――――

③「管理している DNS サーバ」の Forwader に「内部用 DNS サーバ」を指定します。

（「管理している DNS サーバ」が学内からの名前問合せの回答ができる状態にするためです。）

④学内 PC で「管理している DNS サーバ」を直接指名している PC があれば「内部 DNS サーバ」に変更してもらいます。

――――――　平行運用期間　完了　――――――――――――――――――――

⑤「管理している DNS サーバ」の DNS サーバ機能を停止します。

※上記の設定を行うと、以下のような影響があります。

「管理している DNS サーバ」が行っていた問合せは、「外部 DNS サーバ」が行うことになります。「管理している DNS サーバ」が DNS アンプ攻撃・DNS ポイズニング攻撃に対する備えをする必要がなくなります。

新たに Web サーバ等（コンテンツサーバ）を構築する場合、「外部 DNS サーバ」にレコードを追加する必要があるため、KUDOS に申請書を提出していただく必要があります。

以上となります。ご検討をよろしくお願い致します。

【問合せ先】

総合情報システム部（KUDOS）
内線：3450　　メールアドレス：kudos_support@ml.kindai.ac.jp