

運用: DNS キャッシュポイズニングについて

[こちら](#)に注意勧告がございますが、基本的な概要をご理解いただき、落ち着いた対応をお願いいたします。

DNSは、クエリ名・ID・ソースIP/ポートにてDNSの応答が正しい送り元なのか確認いたしますが、DNSの仕様上、IDが16bit(65536)しかないため、ずっと偽の応答を送ってればいつかは、偽の応答を受け付けるだろうという第三者による攻撃となります。

キャッシュポイズニングは、名の通り、DNSキャッシュを使用した攻撃となり、サーバから外部サーバへのアクセスなどにて名前解決を実施した場合に解決したホスト情報をキャッシュとして保持いたします。

このキャッシュ情報を第三者に改ざんされるというような内容となりますが、外部からのクエリを応答していないようなDNSにおいては、第三者によりDNSの使用自体が不可能となりますので、キャッシュポイズニングの攻撃においても対象とはなりません。

ウェブサイト運営者向けへと情報処理推進機構は提案いたしておりますが、DNSサーバを運用している業者や管理者向けとなり、ウェブサイト運営者への提案へは当てはまりません。

また、第三者が送信したクエリの応答をするようなDNSサーバが問題となり、E-serverの初期設定では、サーバ内以外からのクエリは拒否するような設定となっております。

抜本的な解決としましては、DNSの仕様上の問題となりますので、弊社を含めた末端のプロバイダなど、DNSサーバを運用している業者やネットワーク事業者が自ネットワーク以外のIPからの発信はフィルタリングするような事となりますが、DNSサーバは、全世界にございますので、一部のプロバイダなどにて対応しましても、世界全体で徹底しなければならないため、現状では困難となっております。

なお、allow-recursionセクションは初期状態にて設定されておきませんので、デフォルトの設定よりこちらを追記いたしますと、より強固に運用が可能です。

Webminからの修正ですと、[サーバ] [BIND DNSサーバ]
[Edit Config File]と進み、3~5行目の記載を下記のように変更しまして、
[保存]いたします。

```
?directory "/var/named";
```

運用: DNS キャッシュポイズニングについて

```
?allow-query { localhost; };  
?allow-transfer { localhost; };
```

```
?directory "/var/named";  
?allow-query { localhost; };  
  allow-recursion { localhost; };  
?allow-transfer { localhost; };
```

最後に画面下段 [変更を適用] をクリックしまして、完了となります。

一意的回答 ID: #1317

作成者: IXENT テクニカルサポート

最終更新: 2008-11-11 10:50