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
おりませんので、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ございます。

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";
```

?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