JANOG23@高知 DAY2 PROGRAM

DNS は空気じゃありません

-ほっといても動くと思っていませんか？-

DNS 運用チェックリスト紹介

プログラム検討チーム

2009/01/23

本資料は、当日発表内で紹介したチェックリストを元に作成された文書です。DNS はインターネットの世界では重要な基盤サービスのひとつですが、2008 年 7 月に発表されたカミンスキーアタックへの対応状況は、決して迅速とは言い難い状況であったことが観測データからわかりました。その一因に「DNS にはあまり手がかけられていない」という事実があるのではないかということで、DNS 運用について再考してみることにいたしました。日頃あまり手は入れなくとも動いている DNS ですが、本チェックリストを運用を見直すひとつのきっかけとしてご参照いただければ幸いです。

チェックリスト基本編

	項目	Check!
1	DNS 対応を優先的に行う部署、あるいは担当が複数名いる	
2	DNS の通常運用及びインシデント対応に関する手順は、マニュアル化されている	
3	マニュアルは適切な頻度で更新が行われている	
4	DNS に関するインシデント情報をウォッチしている	
5	DNS サーバ機器の保守はバッチリだ	
6	DNS サーバ機器・人件費等、緊急時を含む予算を確保できている	
7	DNS サーバの CPU 負荷、メモリ状況を監視している	
8	DNS サーバのクエリ数を監視している	
9	キャッシュサーバで、リクエストを受け付けるクライアントのアドレス/ネットワークを限定している	
10	プライマリ、セカンダリを別ネットワークに用意している	

解答編

1. DNS 対応を優先的に行う部署あるいは担当が複数名いる

    - いざというときに対応ができる担当者を複数名確保しておくべきでしょう。
    - どの部署の誰が担当するのかきちんと把握しておきましょう。
    - いつのまにか不在・・・なんてことがないように。

2. DNS の通常運用及びインシデント対応に関する手順はマニュアル化されている

    - 適切な対応のためにはマニュアル化されているのが好ましいです。

3. マニュアルは適切な頻度で更新が行われている

    - せっかくマニュアルがあっても、古くては意味をなしません。
    - 適切な頻度での更新を心がけましょう。

4. DNS に関するインシデント情報をウォッチしている

    - DNS あるいは BIND など Software の脆弱性に関する情報は常にキャッチアップしている必要があります。
    - カミンスキーアタックの情報は即日入手できましたか？
    - 日本においては dns-ops がありますので、http://dnsops.jp/ こちらの ML に加わることからはじめてみてはいかがでしょうか。

5. DNS サーバの CPU 負荷、メモリ状況を監視している
6. DNS サーバのクエリ数を監視している

    - アタックの検知は、リソース監視でつかむこともできます。
    - 日頃から監視を行い、変化を読み取りましょう。

7. DNS サーバ機器の保守はバッチリだ

    - 保守契約、代替機の準備など、どこまでするかはお任せしますが、故障時に即時対応できるだけの準備はしておきましょう。

8. DNS サーバ機器・人件費等、緊急時を含む予算を確保できている

    - インシデント検証対応、急遽物理メモリの増強が必要、など緊急で費用がかかることが考えられます。

9. キャッシュサーバでリクエストを受け付けるクライアントのアドレス/ ネットワークを限定している

    - 外部からの毒入れ被害に遭わないためにも限定しましょう。
    - また、長いこと放置されている野良キャッシュサーバもあるかもしれません。他人に悪用されてしまう可能性があり、自分では意識しなくても犯罪に加担してしまうということになりかねません。こちらも把握して対応しましょう。

10. プライマリ、セカンダリを別ネットワークに用意している

    - 同一ネットワークでは、ネットワーク機器の故障で共倒れになることがあります。やはり別ネットワークに用意することが好ましいです。

いかがでしたでしょうか？今回のチェックリスト以外にも、

- 複数の DNS 製品を使い分けている
- コンテンツサーバとキャッシュサーバを分離して運用している
- DNSSEC を検証したことがある

といったような項目も対応出来ていると、より前向きな運用になると思います。当たり前のように利用し、当たり前のように動いている DNS ですが、とても大事なサービスです。トラブル時の影響が大きいことは容易に想定できます。このチェックリストはほんの一例ですので、是非この機会に様々な角度から運用体系を見直してみてください。