ランダムサブドメイン攻撃について
ドメイン名登録者が出来ること

DNS Summer Day 2023
2023/06/23

GMOインターネットグループ株式会社
永井祐弥

(Version 1.1, 最終更新日 2023/06/26)

本日のテーマ

ランダムサブドメイン攻撃などの脅威から
ドメイン名登録者が実施可能な対策について考える

- 2023年に入りランダムサブドメイン攻撃が活発化している
弊社の権威DNSサーバでも増加傾向にあることを観測

- この攻撃手法は以前から存在するが
今一度どういう攻撃手法なのか振り返り
ドメイン名登録者が出来る対応策について考える

ドメイン名登録者（Registrant）

ドメイン名を登録申請する個人名や、企業や団体などの組織名

- 組織内では「代表者」「責任者」「担当者」などの役割が存在する
- レジストリ、レジストラに登録されている情報は申請時のものであるため実際の登録者と異なる場合がある…

GMO.JPの登録情報(WHOIS)

```
Domain Information: [ドメイン情報]
[Domain Name]                   GMO.JP

[登録者名]                      ＧＭＯインターネット株式会社
[Registrant]                    GMO Internet, Inc.

[Name Server]                   ns1.cf.gmointernet.jp
[Name Server]                   ns2.cf.gmointernet.jp
[Signing Key]

[登録年月日]                    2001/05/21
[有効期限]                      2024/05/31
[状態]                          Active
[最終更新]                      2023/06/01 01:05:07 (JST)
```

ネームサーバ（Name Server）

ドメイン名の利用にはネームサーバ（権威DNSサーバ）が必要

- ドメイン名の登録時にオプションで利用出来る場合が多い
- ネームサーバにゾーン（ドメイン名）とDNSレコードを設定する
- 本資料では「権威DNSサーバ」を登録者観点に合わせて「ネームサーバ」で統一する

ネームサーバは変更可能

- PCやスマートフォンと同様に、ネームサーバにも機能、性能が存在する
- ネームサーバを見直すことが対策への第一歩となる

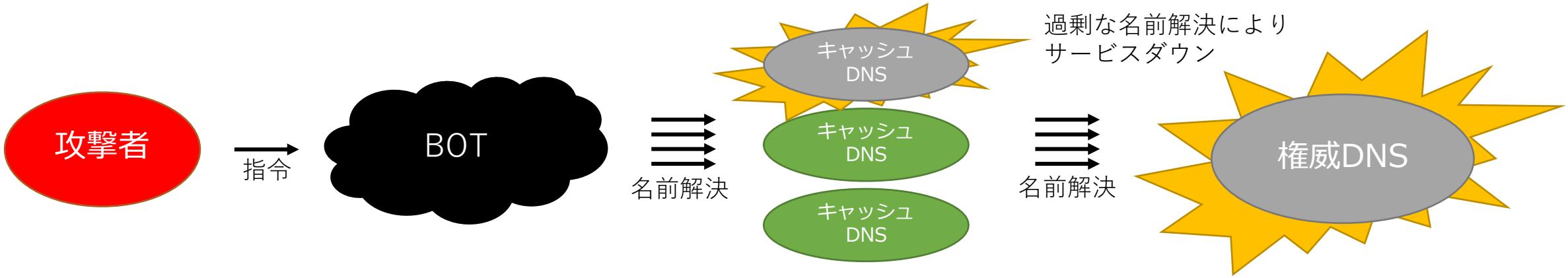
GMO.JPの登録情報(WHOIS)

```
Domain Information: [ドメイン情報]
[Domain Name]                   GMO.JP

[登録者名]                      ＧＭＯインターネット株式会社
[Registrant]                    GMO Internet, Inc.

[Name Server]                   ns1.cf.gmointernet.jp
[Name Server]                   ns2.cf.gmointernet.jp
[Signing Key]
```

ランダムサブドメイン攻撃のおさらい (1/2)

2014年初頭（1～2月頃）から世界的に観測され始めた
DNSサーバを標的としたDDoS攻撃の手法

特徴	ランダムなサブドメインの名前解決（DNSクエリ）を攻撃対象となる ネームサーバへ過剰に送りつけることでサービス停止に追い込む
	キャッシュDNSサーバが未対策の場合、攻撃の影響を受ける可能性もある
	このランダムなサブドメインを用いた攻撃手法は別名「DNS水責め攻撃」 「ランダムプレフィックス攻撃」とも呼ばれる

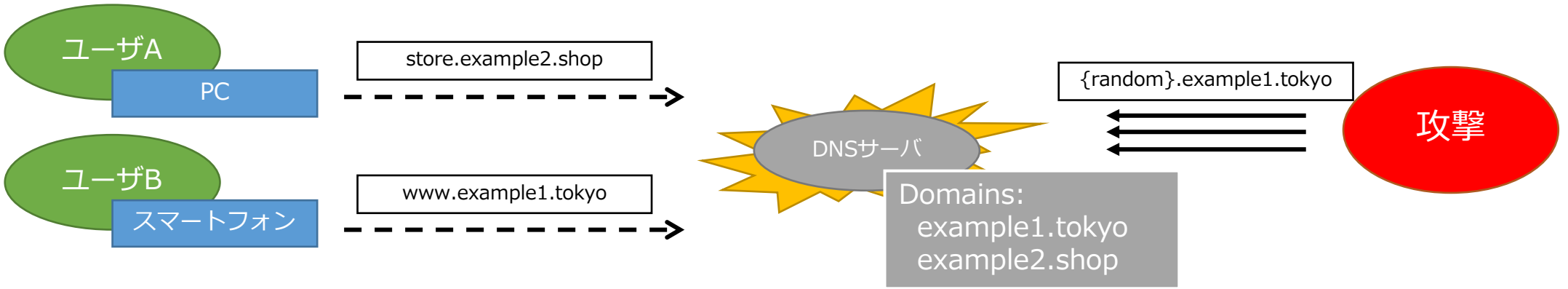


ランダムサブドメイン攻撃のイメージ

ランダムサブドメイン攻撃のおさらい (2/2)

ランダムサブドメイン攻撃によりDNSサーバがダウンすると
名前解決に失敗するためWebサイトへのアクセスや
メールの送受信等に影響し、結果として障害が発生する

- ドメイン名のネームサーバがダウンすると同一のネームサーバに
  設定されている他のドメイン名も影響を受ける
- キャッシュDNSサーバがダウンすると名前解決が失敗し
  クライアントとなるPCやスマートフォン、サーバ等が影響を受ける



障害のイメージ

ランダムサブドメイン攻撃のログ

- 実際のネームサーバへのDNSクエリ（一部加工）
- 1秒間に16万クエリ(160,000/qps)の攻撃規模を観測
- 攻撃に使用されたIPアドレスは推定12,000個以上

```
16:33:17.230226 IP [redacted].24.37007 > 157.7.32.53.53: 53245% [1au] CNAME? azure.example.tokyo. (48)
16:33:17.230291 IP [redacted]28.32610 > 157.7.32.53.53: 29569% [1au] CNAME? akamai.example.tokyo. (49)
16:33:17.230323 IP [redacted]14.38074 > 157.7.32.53.53: 26122% [1au] CNAME? VEGa.eXAmPle.TokYo. (47)
16:33:17.230350 IP [redacted].8.59641 > 157.7.32.53.53: 60286% [1au] CNAME? VectOR.EXampLe.TOkyO. (49)
16:33:17.230393 IP [redacted]3.21989 > 157.7.32.53.53: 15384% [1au] CNAME? lulu.example.tokyo. (47)
16:33:17.230475 IP [redacted]86.47507 > 157.7.32.53.53: 36114% [1au] CNAME? casa.example.tokyo. (47)
16:33:17.230532 IP [redacted]3.8642 > 157.7.32.53.53: 21148% [1au] CNAME? video4.example.tokyo. (49)
16:33:17.230563 IP [redacted].99.64712 > 157.7.32.53.53: 64246% [1au] CNAME? pUsHmAiL.ExAmpLE.tOKyO. (51)
16:33:17.230599 IP [redacted]49.17213 > 157.7.32.53.53: 4777% [1au] CNAME? gj.example.tokyo. (45)
16:33:17.230673 IP [redacted]229.32311 > 157.7.32.53.53: 6944% [1au] CNAME? cookie.example.tokyo. (49)
16:33:17.230724 IP [redacted]54.61533 > 157.7.32.53.53: 17538 [1au] CNAME? accounting.example.tokyo. (53)
16:33:17.230751 IP [redacted]107.39892 > 157.7.32.53.53: 51848 [1au] CNAME? lobby.example.tokyo. (48)
16:33:17.230805 IP [redacted]32.52280 > 157.7.32.53.53: 46459% [1au] CNAME? web6.example.tokyo. (47)
16:33:17.230885 IP [redacted]2.35641 > 157.7.32.53.53: 14367% [1au] CNAME? sv02.example.tokyo. (47)
```

ランダムサブドメイン攻撃の防御手段

ランダムサブドメイン攻撃は通常の名前解決を利用した
DDoS攻撃のため簡易的な対策では効果が弱い

- DNSサーバのパフォーマンスの強化
  - 1つのIPアドレスに対する負荷分散強化（Load Balancer、IP Anycast）
  - 1つのドメイン名に対するネームサーバの追加（DNSサービス、設備追加）
  - 高性能なソフトウェアへの切り替え
- 過剰な名前解決の防止
  - レートレミットなど、過剰な名前解決を制限する設定
  - キャッシュDNSのACL設定見直しや、ボットネットなどの不正利用対策
- ランダムサブドメイン攻撃のブロック
  - DNSに対応したDDoS Mitigation、Protection機能を謳っている製品の導入
  - FWやDNS Load Balancerなどによるパケットベースのフィルタリング

2023年のランダムサブドメイン攻撃 (1/2)

今年初頭以降、国内で複数のネームサーバがダウンする事象が発生

- 原因はランダムサブドメイン攻撃によるものと考えられる
- 弊社のネームサーバにも攻撃が来ていることを観測
- 特に今月（6月）は攻撃の勢いが強い

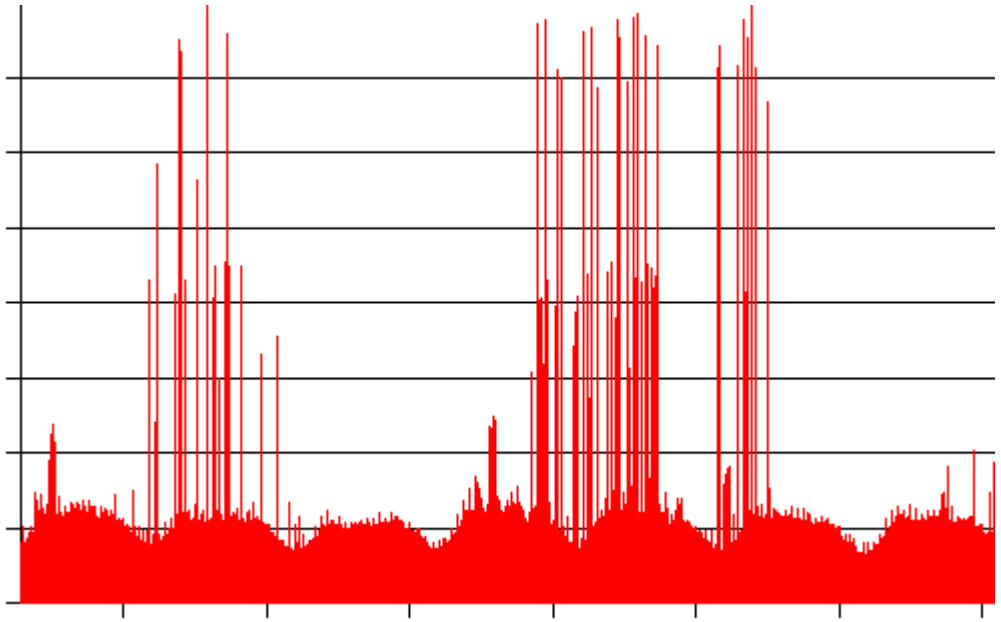
攻撃対象や目的などは不明

- 国内で広く使用されているドメイン名が対象に追加された可能性が高い
- 自治体や著名なドメイン名が影響を受けたことでニュースにも
- これまでにもランダムサブドメイン攻撃は不定期的に発生していたが、未対策のネームサーバが狙われた事で影響が出たと考えている
- クラウドサービスなどでは従量課金による請求となるため注意が必要
- 現時点でも攻撃が続いているため引き続き警戒が必要

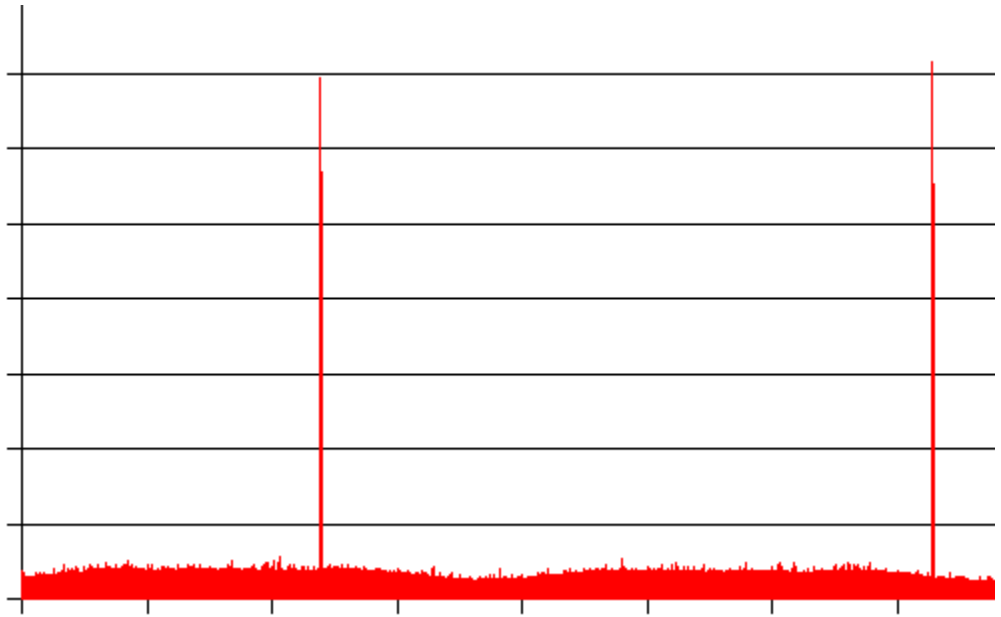
2023年のランダムサブドメイン攻撃 (2/2)

実際に弊社で観測したランダムサブドメイン攻撃

- 数値などは当日会場にて



ある1週間のグラフ



ある1日のグラフ

ドメイン名登録者として考えるべき事項

1. 優先順位の決め方
2. ネームサーバの選択
3. TTL値の見直し
4. ゾーンファイルのバックアップ
5. 緊急時の対応手順
6. やっぱり監視

1. 優先順位の決め方

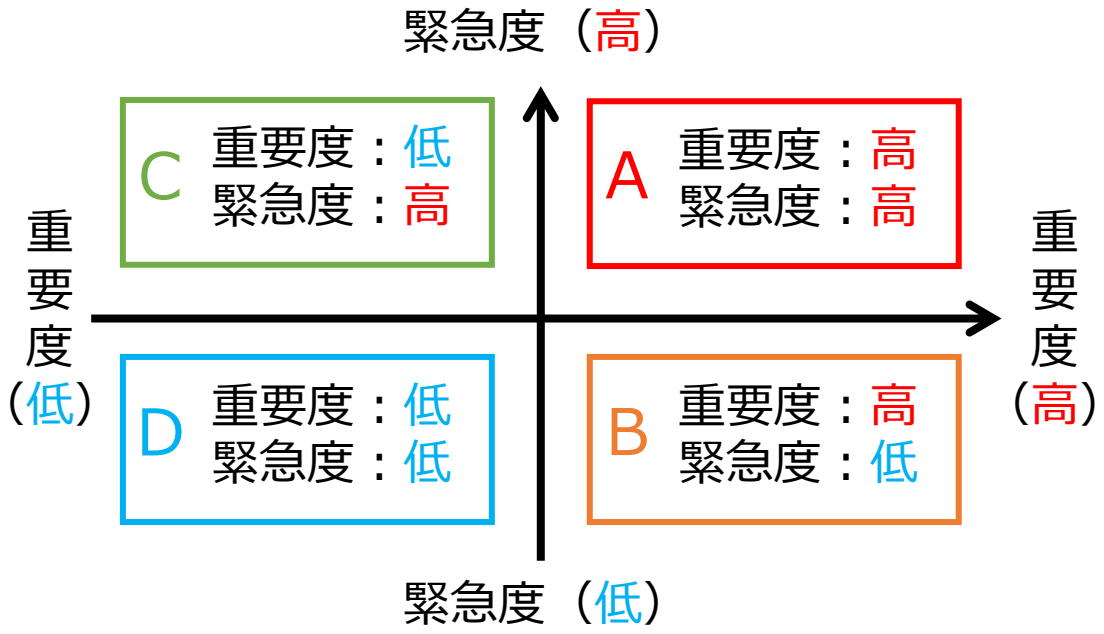
緊急度、重要度のマトリクスで考える

A) 対応しなければならない（MUST）
- サービス停止が致命的な影響を受ける
- 人命に関わる、社会責任が問われる

B) 対応するべき（SHOULD）
- サービス停止が重大な影響をうける
- 事業に影響する、損害が発生する

C) 対応を推奨（RECOMMENDED）
- サービス停止による影響が比較的小さい
- ABが存在しなければ対応する

D) 対応してもよい（MAY）
- サービス停止による影響が小さい
- ABCが存在しなければ対応を検討する



1. 緊急度,重要度のマトリクス

AとDのケースは問題にならない

- 緊急度、重要度が高いドメイン名は既に対応されているか、対応を進めていると考えられる
- 緊急度、重要度が低いドメイン名は対応の優先度も低い

BとCは優先順位を混合しやすいため注意が必要

- インターネット上の事業で使用するドメイン名はB（対応するべき）のケースに該当すると考えられる
- 重要度で判断する
  - サービス障害発生時に影響があるなら、重要度が高いと言える
  - サービス障害発生時に影響がない、攻撃が停止するなど時間経過で復帰するのであれば重要度は低いと言える

A (MUST)
重要度：高
緊急度：高

B (SHOULD)
重要度：高
緊急度：低

C (RECOMMEND)
重要度：低
緊急度：高

D (MAY)
重要度：低
緊急度：低

2. ネームサーバの選択 (1/2)

ドメイン名登録者はドメイン名の登録申請と
ネームサーバの用意をそれぞれ行う必要がある

- ドメイン名の登録申請は取次サービス（レジストラ、リセラ）で行う
- UX向上の一環として、サービスの申込み、ドメイン名の登録申請、ネームサーバを提供している場合が多い
- レンタルサーバなどのホスティングサービスで申込みと同時にドメイン名が利用出来るのは上記のような理由によるもの
  - 土地と建物の関係に似ている

	手順
ドメイン名の登録	取次サービス（レジストラ、リセラ）で登録申請する
ネームサーバの用意	DNSサービスを契約する 取次サービスが提供するネームサーバを利用する

2. ネームサーバの選択 (2/2)

ネームサーバを検討するためには、大きく2つに分類して考える

- 内製：自組織や個人で設計、構築、運用するもの
  （ソフトウェアやアプライアンスなど）
- 外注：DNSホスティングサービスや、他組織などに委託しているもの
  （レンタルサーバや、委託による専用のネームサーバなど）

	検討内容
内製	• 継続した運用は行えるか？ • 設備、機器は老朽化していないか？ • ネームサーバは有効な防御手段を備えているか？ • 外注のネームサーバと併用しなくてもよいか？
外注	• サービスは十分な機能、性能を提供しているか？ • 異なるDNSサービスを併用しなくてもよいか？

2. DNSホスティングサービスのススメ (1/2)

DNSホスティングサービス（外注）

- DNSホスティングサービスの種類
  - レジストラ（リセラ）、ホスティング事業者、ISP、CDN事業者、クラウドサービスなどが提供
- 国内外でIP Anycastを導入しているサービスはレベルが高い
  - 国内はレイテンシを重視
  - 海外はDDoS攻撃の吸い込み先として
  - ネームサーバはIPv6に対応していると尚良い
- DDoS攻撃対応を謳っているDNSホスティングサービス
  - CDN事業者や、クラウドサービスなどが提供している
  - Webサーバと組み合わせて利用する場合が多いため、費用対効果は高いといえる

2. DNSホスティングサービスのススメ (2/2)

DNSホスティングサービスの多様性

- DNSホスティングサービスの性質上、
  他ドメイン名への攻撃の巻き添えに遭う恐れがある
- 複数のDNSホスティングサービスを併用することで
  何れかのネームサーバがダウンしても生存出来る可能性が高まる

```
example.tokyo.      86400   IN   NS   ns1.example.tokyo.
example.tokyo.      86400   IN   NS   ns2.example.tokyo.
example.tokyo.      86400   IN   NS   ns-a1.example.com.
example.tokyo.      86400   IN   NS   ns-a2.example.com.
example.tokyo.      86400   IN   NS   01.example.jp.
example.tokyo.      86400   IN   NS   02.example.jp.
```

内製

外注（A社）

外注（B社）

2. ネームサーバにおける防御手段と性能について

- 明確な基準は無い...
  - しかし万全であることが要求される

- 個人的な所感としては一定以上の性能（例えば1,000,000/qps）やDDoS Mitigation、Protection機能などは必要だと考える

- ネームサーバが1つしか登録されていない場合や1つのネームサーバが10,000/qpsに耐えられないなど性能が著しく低い場合は、緊急度が高いと言える

- 外注するDNSサービスの選定にはDNSOPSで活動している「権威DNSサービス調査報告（仮）」などを参考にすると良い

3. TTL値の見直し

DNSレコードのTTL値は適切なものを設定する

```
example.tokyo.     10     IN     A     192.0.2.123
```

	短いTTL値	長いTTL値
障害発生時	すぐに名前解決出来なくなる	徐々に名前解決出来なくなる
DNSレコードの更新	体感的に反映が早い	体感的に反映が遅い
ネームサーバへのクエリ数	多くなる	少なくなる

障害回復までのシナリオを検討する

- 名前解決が失敗してから、障害が回復するまでの時間
- DNSレコードの更新に必要な本当の時間
- CDNやクラウドサービスなどで短いTTL値を設定しているのは
  DNSレコードの更新を含めてシステムが自動化されているため

4. ゾーンファイルのバックアップ

ゾーンファイルのバックアップは必ず用意する

- 緊急時にゾーンファイルが無くて何も出来ないのは避ける
- 緊急時でもアクセス可能な場所に保管する（稼働中のサーバはNG）
- 内製の場合はバックアップを自動化するとよい（可能なら世代管理する）
- 外注の場合は手元にも必ずバックアップを保存し
  ゾーンファイル（DNSレコード）を更新する都度バックアップも更新する

マスタ/スレーブ構成の場合はマスタのサーバを隠避する

- 隠しマスタ（Hidden Master）はスレーブへのゾーン転送のみ行い
  外部には公開しない

バックアップしたファイルは定期的に点検する

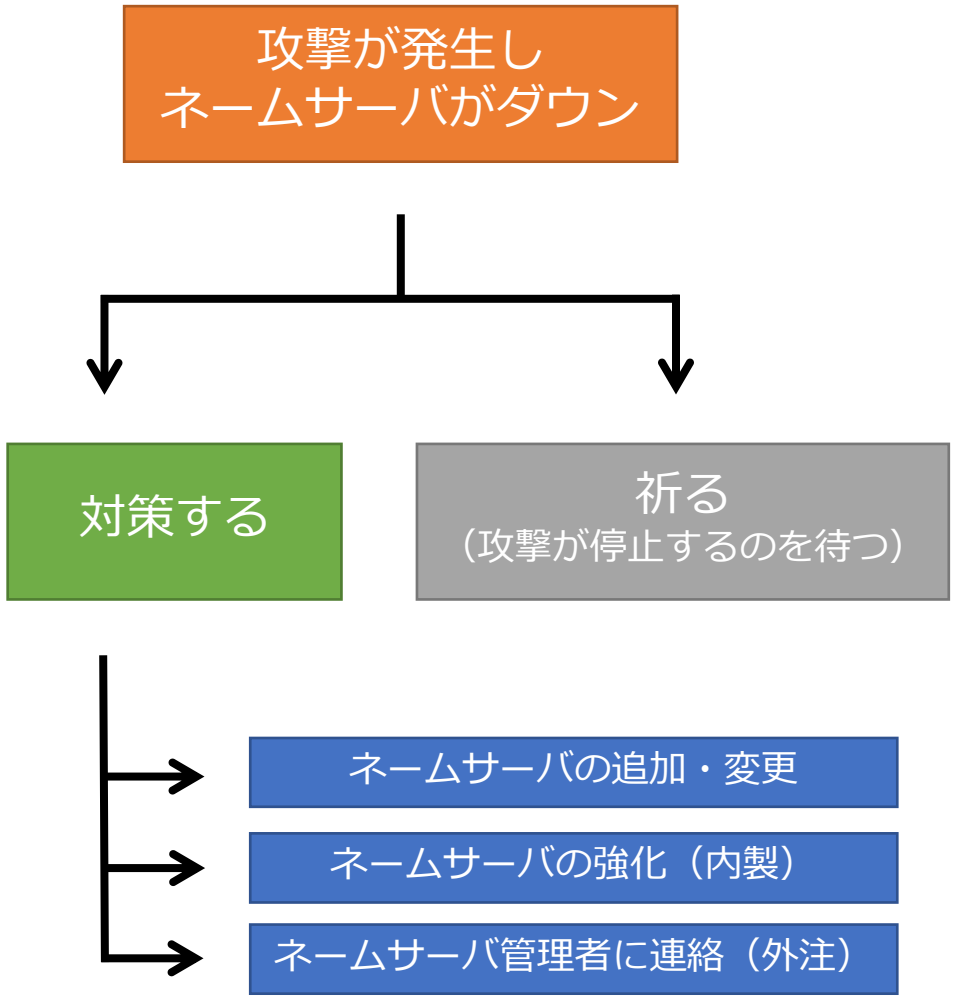
- バックアップが失敗していないか、内容が不足していないか確認する

5. 緊急時の対応手順

緊急時の手順書を用意する
- DNSレコードの変更方法
- ネームサーバの変更方法

緊急時のシナリオを作成する
- システムがダウンしたときに
  どのタイミングで何を判断するべきか？
- 対応が複数人でも正しく連携出来るか？
- 不必要な待ち時間が発生しないか？

1年毎に定期訓練する
- いざ実施すると上手く行かない場合がある
- 手順は毎年見直す（アップデート）



6. やっぱり監視

ドメイン名の監視はネームサーバに対して行う

- ネームサーバを監視することでサービスダウンに素早く対応出来る
  - 緊急時の対応手順を活用する
- 監視を設定する時はインターバル（頻度）に注意
  - 監視のやりすぎでDoS攻撃にならないように注意する
  - 重要度が高ければ数十分から数時間程度の頻度で
  - 重要度が低ければ1日1回でも十分
- 重要なドメイン名ではNSレコードの監視も行う
  - 予期しないネームサーバ変更の検知
  - 同じネームサーバで大量の監視は要注意（DoS攻撃になる恐れ）

まとめ

ランダムサブドメイン攻撃の脅威

- 予告なく、突然やってくる
- 現在続いている攻撃は中長期的に長引く可能性もある
    - 特に今月は攻撃パターンに変化があり、勢いも強い
- DNSサーバの対策は今まで以上に求められる

ドメイン名登録者が出来る対策

- 優先順位を明確に決めよう
- ネームサーバや、TTL値を定期的に見直そう
- 不測の事態に備えてバックアップ、手順を徹底しよう
- 監視も大切
- ドメイン名を大事にしよう

おまけ

おまけ

以下のワードは当日会場にて...

- PowerDNS
- Open Resolver
- Public DNS

改訂履歴

- v1.0：初版作成
- v1.1：質疑応答にて頂きましたコメントを本資料に反映しました

すべての人にインターネット

GMO