マネージドサービス時代の DNSの運用管理について考える

～ DNSテイクオーバーを題材に ～ ランチのおともにDNS

2021年7月9日

Internet Week ショーケース オンライン 2021

株式会社日本レジストリサービス（JPRS）

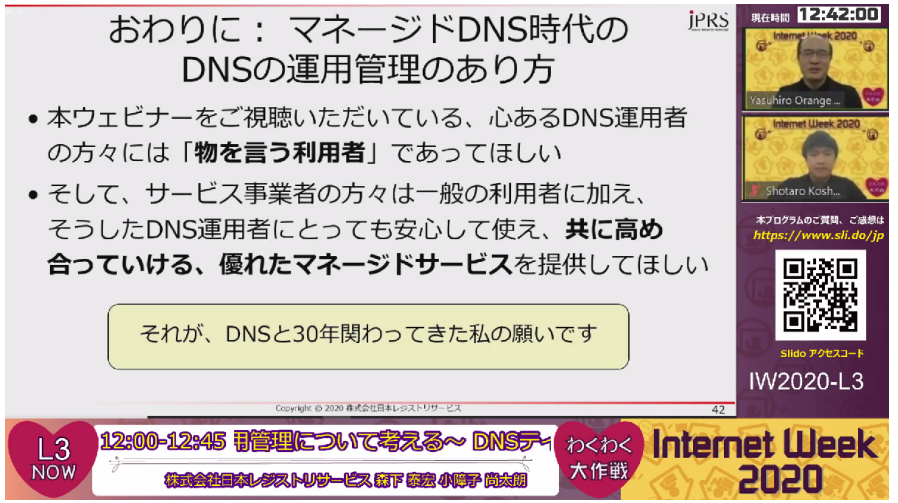
森下 泰宏

本セミナーはInternet Week 2020 ランチタイムウェビナーのUpdate版です

ランチのおともにDNS

- JPRSではInternet Week 2007より、ランチセミナーをご提供
  - ランチ（お弁当）
  - DNSに関する旬の話題
- Internet Weekのオンライン化に伴い、 2020年は「ランチタイムウェビナー」をご提供

Internet Week 2018でご提供したお弁当



ショーケースでも「ランチのおともにDNS！」

- 今回のInternet Week ショーケースではアンケートにお答えいただいた皆様に、コーヒーギフトをご提供
  - 後日、ギフトチケットを送付いたします

giftee コーヒーギフト
<https://giftee.biz/consumer/coffee_gift/>

- DNSのお話に耳を傾けつつ、それぞれのランチタイムをお楽しみいただければ幸いです！

講師自己紹介

- 森下 泰宏（もりした やすひろ）
  - 所属：JPRS 技術広報担当・技術研修センター
  - 主な業務内容：技術広報活動全般・社内外の人材育成

＜略歴＞

1988年	独立系SIerに入社 1990年よりWIDE Projectメンバーとして、 日本のインターネット構築に創始期より参加。
1993年	学校法人東京理科大学情報処理センター着任 キャンパスネットワーク及び教育用システムの設計、 構築、運用を行う。
1998年	社団法人日本ネットワークインフォメーションセンター（JPNIC）着任 JPドメイン名登録システム及びJP DNSの管理運用に従事。
2001年	株式会社日本レジストリサービス（JPRS）に転籍 DNSに関する技術研究を中心に活動。
2007年	同社技術広報担当として、 DNSおよびドメイン名関連技術に関するプロモーション全般を中心に活動中（現職）。
2021年	同社技術研修センター主任講師として、教育・研修を通じた社内外の人材育成を担当（兼務・現職）。

本日の内容

1. DNSテイクオーバーの概要と類似する攻撃手法との違い
2. 最近のインシデント事例と防止策
3. マネージドDNS時代のDNSの運用管理のあり方

1. DNSテイクオーバーの概要と類似する攻撃手法との違い

DNSテイクオーバーとは?

- テイクオーバー（takeover）＝ 引き継ぐ
- DNSの仕組みを利用して、**登録者が意図しない形で**
  ドメイン名の利用を引き継ぐ行為
- IETFで標準化された用語ではない

DNSテイクオーバーの分類

- **攻撃方法**による分類
  1. ドメイン名の登録情報を書き換える
  2. DNSの設定ミスに付け込む
  3. ドメイン名の更新ミスに付け込む
- **ドメイン名の状態**による分類
  a. 使用中のドメイン名
  b. 使用を終了したドメイン名

攻撃方法＼ドメイン名の状態	a. 使用中のドメイン名	b. 使用を終了したドメイン名
1. ドメイン名の登録情報を書き換える	1-a	1-b
2. DNSの設定ミスに付け込む	2-a	2-b
3. ドメイン名の更新ミスに付け込む	3-a	3-b

DNSテイクオーバーの分類

- 以降では、 **DNSの設定ミス**に付け込み、**使用を終了したドメイン名**の利用を引き継ぐ、**サブドメインテイクオーバー**と**NSテイクオーバー**に注目（分類表の**2-b**）

サブドメインテイクオーバーとは?

- 外部サービスの利用開始時に設定したサブドメインの設定が**利用終了後も残ったままになっている**ことを利用し、そのサブドメインの引き継ぎ（テイクオーバー）を図る攻撃手法
- 自ゾーンに残ったままになっている、CNAMEレコードやA/AAAAレコードが狙われる
  - 以下は、example.jpゾーンに設定されるCNAMEレコードの例

```
campaign.example.jp. IN CNAME cdn.example.net.
```

NSテイクオーバーとは?

- 外部サービスの利用開始時に設定したネームサーバー設定が**利用終了後も残ったままになっている**ことを利用し、そのドメイン名の引き継ぎ（テイクオーバー）を図る攻撃手法
- 親ゾーンに残っているNSレコードが狙われる
  - 以下は、jpゾーンに設定されるNSレコードの例

```
example.jp.  IN NS ns-99.example.net.
             IN NS ns-999.example.org.
```

サブドメインテイクオーバーと NSテイクオーバーの共通点・相違点

- 共通点：**残ったままになっているDNS設定を利用**し、**使用を終了したドメイン名**を使われる
- 相違点：狙われるリソースレコードが異なる
  - サブドメインテイクオーバー：**自ゾーン**の**CNAME**や**A/AAAA**
  - NSテイクオーバー：**親ゾーン**の**NS**

```
campaign.example.jp. IN CNAME cdn.example.net.
```

```
example.jp. IN NS ns-99.example.net.
            IN NS ns-999.example.org.
```

Dangling records

- こうした、利用終了後も残ったままになっている
  リソースレコードは「**dangling records**」と呼ばれる
  - dangling = 宙ぶらりんの
- DNS運用における**脅威（threat）**となる

CNAMEの参照先に
campaign.example.jpの
実体が存在しない

```
campaign.example.jp. IN CNAME cdn.example.net.
```

```
example.jp. IN NS ns-99.example.net.
            IN NS ns-999.example.org.
```

NSの参照先に
example.jpゾーンが
存在しない

DNSテイクオーバーと類似する攻撃手法との違い

- ここでは、DNSテイクオーバーと以下の二つの攻撃手法との違いについて説明
- ドロップキャッチ
  - 廃止したドメイン名が一時凍結期間を経て、誰でも登録できる状態になる瞬間を狙って再登録を図る行為
- ドメイン名ハイジャック
  - ドメイン名の管理権限を持たない第三者が、ドメイン名を自身の支配下に置く行為

DNSテイクオーバーと ドロップキャッチの共通点・相違点

- 共通点：いずれも、**使用を終了したドメイン名**が標的になる
- 相違点：ドロップキャッチでは、**ドメイン名の更新ミス**に付け込む

攻撃方法 ＼ ドメイン名の状態	a. 使用中のドメイン名	b. 使用を終了したドメイン名
1. ドメイン名の登録情報を書き換える	1-a	1-b
2. DNSの設定ミスに付け込む	2-a	2-b
3. ドメイン名の更新ミスに付け込む	3-a	3-b

DNSテイクオーバーの分類

DNSテイクオーバーは2-b
ドロップキャッチは3-b

DNSテイクオーバーと ドメイン名ハイジャックの共通点・相違点

- 共通点：いずれも、**第三者にドメイン名を使われる**ことを示す用語として使われている
- 相違点：ドメイン名ハイジャックは、**使用中のドメイン名の管理権限を奪う**というニュアンスで使われる場合が多い

攻撃方法＼ドメイン名の状態	a. 使用中のドメイン名	b. 使用を終了したドメイン名
1. ドメイン名の登録情報を書き換える	1-a	1-b
2. DNSの設定ミスに付け込む	2-a	2-b
3. ドメイン名の更新ミスに付け込む	3-a	3-b

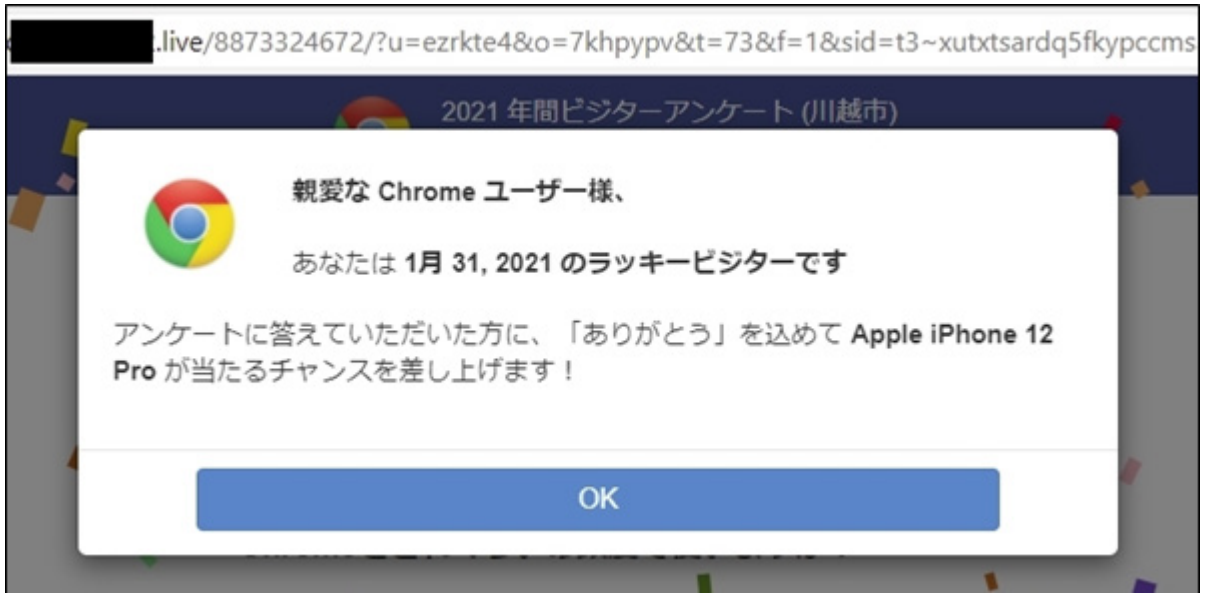
DNSテイクオーバーの分類

DNSテイクオーバーは2-b
ドメイン名ハイジャックは1-a～3-a

2. 最近のインシデント事例と防止策

インシデント事例①：iPhone当選詐欺

- 画面に突然「iPhoneが当選した」旨の画面が表示
- アンケートと共に、アカウント情報・クレジットカード情報などの入力を促し、情報を窃取
- **検索で表示されたWebサイト**（おとりサイト）から、複数回のリダイレクトを経由して、詐欺サイトに誘導



おとりサイトの作成に
サブドメインテイクオーバーを利用

- 著名企業・自治体などのサブドメインをテイクオーバーし、検索結果に表示されるおとりサイトを作成
  - 作成には、サブドメインテイクオーバー以外も使われた模様
- 著名なドメイン名や政府関係のドメイン名を使うことで、**検索で上位に表示される**ことを期待していたと考えられる
- 国内外の複数のドメイン名が被害に
  - 2020年7月までに、100件以上の被害事例を確認
  - 日本の上場企業のドメイン名も含まれている

インシデント事例②：偽サイトの作成

- サブドメインテイクオーバーされたドメイン名：
  demo.pref.[redacted].lg.jp（ある県のLG.JPドメイン名のサブドメイン）
- 被害に遭ったサイト：[redacted].com（著名なゲームの攻略サイト）
- 放置されたCNAMEレコードの参照先に、同じ名前でサイトを作られた

```
demo.pref.[redacted].lg.jp. IN CNAME ep-[redacted]-local.azureedge.net.
```

  - 攻撃者がMicrosoft Azure上に、同じ名前でサイトを作成

アフィリエイト情報付き

- 攻撃者が本物のコンテンツをコピーして偽情報を混ぜ、偽サイトを作成
  - **ゲームに登場するキャラクターの名前で検索した際に、偽サイトを本物より上に表示させることに成功**

一時的に、 demo.pref.[redacted].lg.jpが[redacted].comよりも上に表示される状態だった

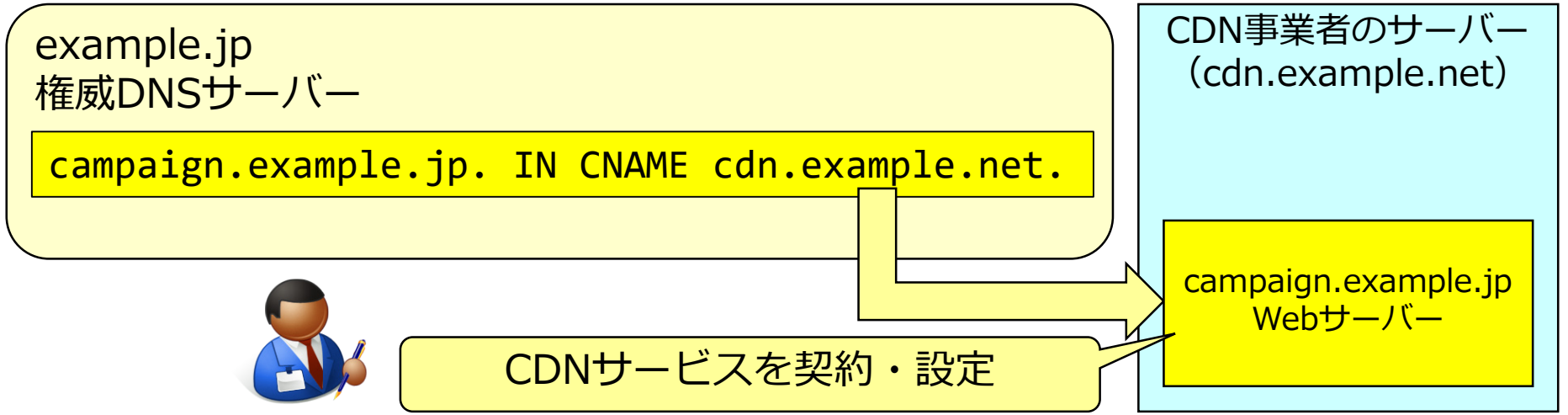
サブドメインテイクオーバーが発生する流れ（1/3）

① キャンペーンなどで、期間限定のサイトを公開

– 外部のCDN（Content Delivery Network）サービスを利用

- cdn.example.netで運営されるCDNサービス上にサイトを構築、CNAMEレコードを設定

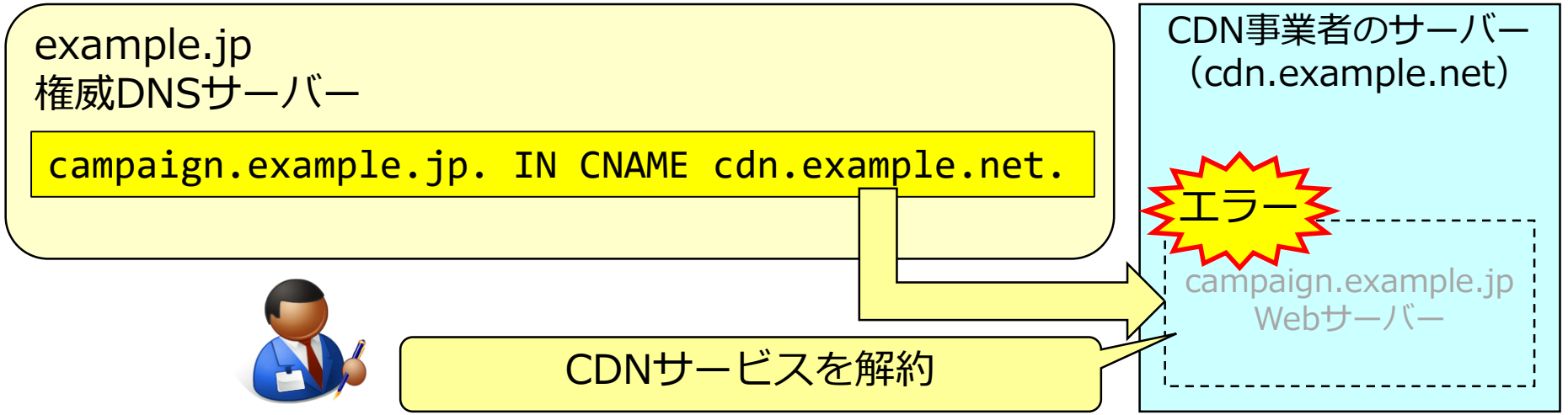
– campaign.example.jpというドメイン名で、Webサイトを公開



サブドメインテイクオーバーが発生する流れ（2/3）

② キャンペーンが終了、CDNサービスを解約

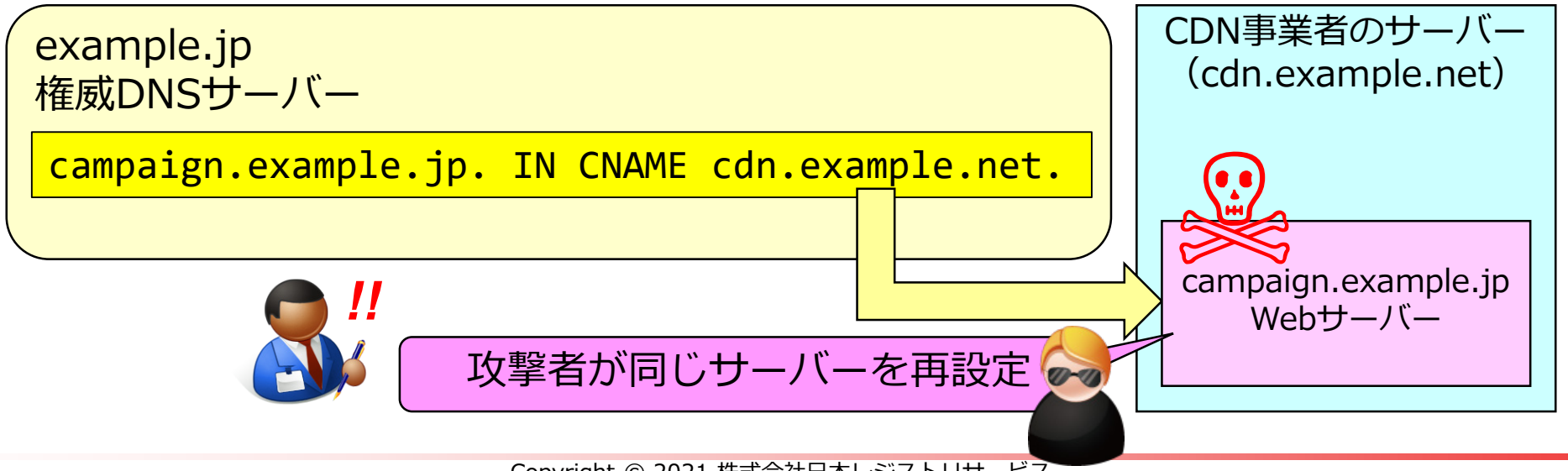
- 事業者側の設定を削除、Webサイトにアクセスできない状態に
- 設定したCNAMEレコードは残ったまま
  - 削除の必要があることを認識していない or 削除を忘れている



サブドメインテイクオーバーが発生する流れ（3/3）

③ 攻撃者が攻撃可能なサブドメインを発見、サブドメインテイクオーバーを実行

- CDNサービス上に、同じドメイン名のサーバーを再設定
- 設定したWebサーバー上で、コンテンツを公開

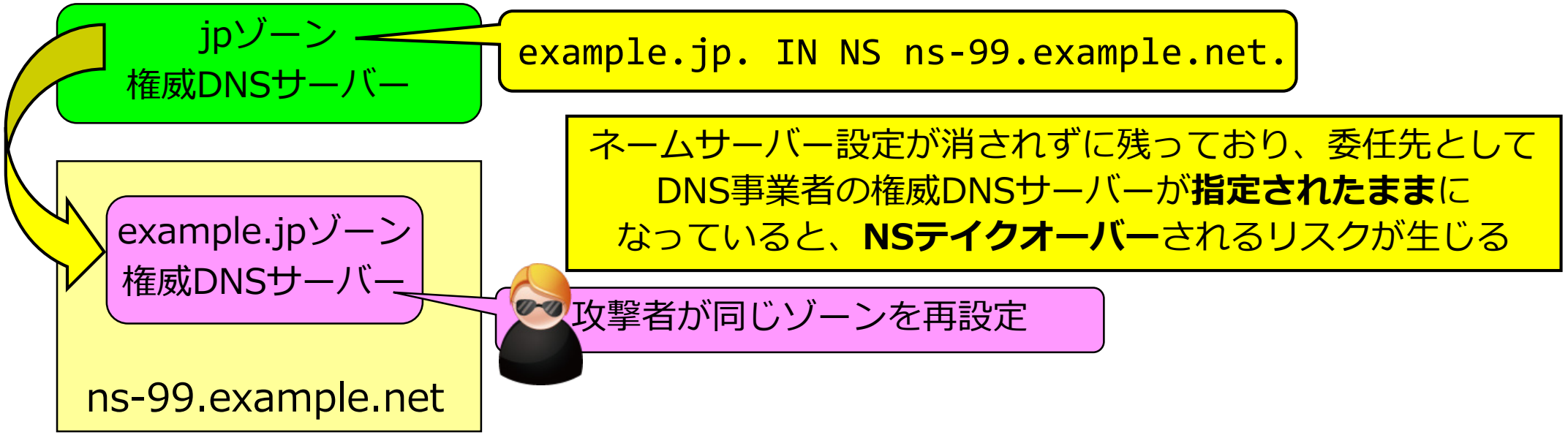


サブドメインテイクオーバーのリスク

- 使用していないサブドメインであっても、テイクオーバーされた場合のリスクは高い
- 考えうるリスクの例
  - フィッシングサイトの作成
  - クッキーの改変
  - 成り済ましメールの発信
  - サーバー証明書の不正取得、など
- **親ドメインのテイクダウン**を狙った、Abuse行為もありうる
  - 親ドメインに対するDoS攻撃が可能になる

NSテイクオーバーにも注意が必要

- 使用休止中のドメイン名のネームサーバー設定を悪用
  - サブドメインテイクオーバーと同様の仕組みで、ドメイン名をテイクオーバー可能



攻撃者は攻撃対象を どのように発見するのか?

- サブドメインテイクオーバー・NSテイクオーバーが可能な状態は、外部からのDNS検索で発見可能
- 攻撃対象を発見するためのツールがインターネット上で公開
  - 総当たり検索（enumeration）を高速に実行し、dangling recordsを発見する

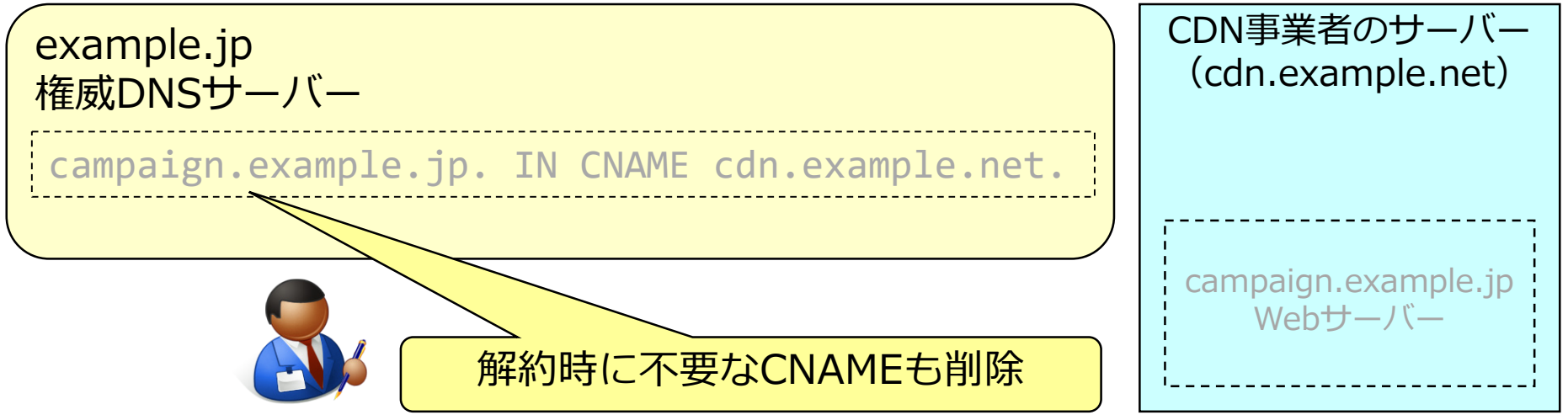
ポイント：攻撃と同じ方法で、防御も可能になる

サブドメインテイクオーバー・NSテイクオーバーの対策

- 利用者ができる対策と、サービス事業者ができる対策がある
- **利用者**ができる対策の例
  - 外部サービスの使用終了時に、**DNS設定も削除**する
  - Dangling recordsが**残っていないかチェック**する
- **サービス事業者**ができる対策の例
  - テイクオーバー**されにくい形**でサービスを提供する

利用者ができる対策（1/2）

- 外部サービスの利用終了時に、
  利用開始時に設定した**DNS設定も削除**する
  - 自ゾーンのCNAMEレコード・A/AAAAレコードの削除
  - 親ゾーンのNSレコードの削除



利用者ができる対策（2/2）

- **Dangling recordsが残っていないかチェック**する
  - 事業者が技術文書やチェックツールを公開している場合もある
    - 例：Microsoft Azureのサブドメインテイクオーバーに関する技術文書と、使用中のサービスにdangling recordsがないか確認するチェックツール

未解決の DNS エントリを防ぎ、サブドメインの乗っ取りを回避する
<https://docs.microsoft.com/ja-jp/azure/security/fundamentals/subdomain-takeover>

Find Dangling DNS Records
<https://github.com/Azure/Azure-Network-Security/tree/master/Cross%20Product/Find%20Dangling%20DNS%20Records>

サービス事業者ができる対策

- テイクオーバー**されにくい形**でサービスを提供する
  - 一部の事業者が、以下の対策を実施済み
    - 例1：サーバー証明書を提出しないと、Webサーバーを設定できない
    - 例2：CNAMEレコードを削除しないと、Webサーバーを削除できない

どうすれば、サービス事業者が
こうしたサービスを提供するようになるのか？

3. マネージドDNS時代のDNSの運用管理のあり方

DNSサービスの変化

- DNSサービスの提供・利用の形態は、インターネットそのものや、それを取り巻く状況の変化に対応する形で**多様化・高機能化**してきた
- 権威DNSサーバーのサービスに注目し、これまでの状況を振り返る

①セカンダリサーバーの外部委託

- 商用サービス以前：セカンダリサーバーの持ち合い
  - いわゆる「お友達プロトコル」や、関係が深い組織同士の協力
    - JUNET時代の上流・下流サイトや、関連会社など
- 商用サービスの時代を迎え、
  セカンダリサーバーを請け負う**サービス**が出現

DNSサービスの始まり

②DNSインフラの外部委託

- DNSのインフラと、そのオペレーションを外部に委託
- サービスの例
  - より高い処理能力・大きなネットワーク帯域の提供・利用
  - IP Anycastを用いた広域分散

DNSの「器」を外部委託

③DNSデータの外部委託

- DNSデータの管理を外部に委託
- サービスの例
  - コントロールパネルによるゾーンデータの管理
  - 複数のDNSサービスへのデータのデプロイ
  - ゾーンデータのDNSSEC署名
  - DNSSEC鍵の管理、など

DNSの「中身」を外部委託

④付加サービスの提供・利用

- 事業者が提供する他のサービスとの連携・一体化
- サービスの例
  - DNSを利用した広域ロードバランシング
  - CDNサービス・クラウドサービスとの連携、など

より高機能な「サービス」を提供・利用

まとめ：DNSサービスの変化

- 状況の変化に対応し、提供・利用されるDNSサービスの多様化・高機能化が進んだ
  - ① セカンダリサーバーの外部委託
  - ② DNSインフラの外部委託
  - ③ DNSデータの外部委託
  - ④ 付加サービスの提供・利用

多様かつ高機能なサービスを利用可能な、
マネージドサービスの時代に

DNSサービスの変化と サービス事業者と運用者の関わり

- 提供・利用されるサービスの多様化・高機能化に伴い、各組織の運用者のサービスへの関わりも変化している
- 運用管理における、**権限**と**責任**が分化
  - 運用管理の権限：**外部に委託**する
  - 運用管理の責任：**各組織の運用者**が持つ

関わりの変化に起因する新たなトラブル・インシデント

- 関わりの変化に伴い、サービス利用時・解約時の**運用ミス**や**設定不備**などに起因する、**新たなトラブル・インシデントの発生**が報告されるようになった
- 本ウェビナーで紹介した**サブドメインテイクオーバー**や**NSテイクオーバー**は、その典型例

トラブル・インシデントの発生要因

- マネージドサービス時代を迎え、多様かつ高機能なサービスを、より手軽に利用できるようになった
- しかし、運用管理の権限と責任が分化することで、**運用者が自身の責任を果たせない**状況が見られるようになった

運用者が責任を果たせるようにするためには
どうすればよいか？

マネージドサービス時代の DNSの運用管理のあり方

- 2018年のランチセミナーで提案
  - 運用体制を構築・強化する
    - DNS単体ではなく、組織全体のリスクマネージメントの一環として考える
    - それぞれの関係者・立場で、地道で継続的な活動を進める
- **本ウェビナーで提案**
  - **運用者が責任を果たせるマネージドサービスを提供・利用**する
  - その実現のため、**サービス事業者と運用者がそれぞれの立場で活動・協調**する

サービス事業者がすべきこと（1/2）

- **サービスモデルにおける、トラブル・インシデントのリスク低減**

ポイント：仕組みで防ぐ

- DNSテイクオーバーにおける具体例
  - 例1：設定するドメイン名の管理権限の確認
    - 例：Webサーバーの設定における、サーバー証明書の提出の必須化
  - 例2：設定削除における事前作業実施の確認
    - 例：Webサーバーの削除における、DNS設定の事前削除の必須化

サービス事業者がすべきこと（2/2）

- 運用者にとってわかりやすく、活用しやすい**情報の発信や、支援ツールの提供**

ポイント：運用者の成長を促す

- DNSテイクオーバーにおける具体例
  - テイクオーバーされた際のリスクの説明
  - テイクオーバーを回避するための設定例・運用手法の紹介
  - Dangling recordsをチェック・発見可能なツールの提供、など

運用者がすべきこと

- より安全な、トラブル・インシデントのリスクが低くなるサービスを、サービス事業者に**提供させる**ための活動
- 言い換えると・・・
  - サービス事業者が、安全なサービスを**提供したくなる**活動
- 具体例
  - 例1：サービス事業者への積極的なリクエスト・フィードバック
  - 例2：より安全なサービス事業者の選択（そのためのスキルの取得）

ポイント：サービス事業者の成長を促す

「**物を言う利用者**」になる

サービス事業者と運用者の より緊密な連携・協調

- サービス事業者と運用者における、**より緊密な連携・協調**
- 具体例
  - 利用者コミュニティの設立・活動
    - サービス事業者によるもの
    - 運用者による自主的なもの

双方向性を持つ活動が望ましい

おわりに：マネージドDNS時代のDNSの運用管理のあり方

- 本ウェビナーをご視聴いただいている、心あるDNS運用者の方々には「**物を言う利用者**」であってほしい
- そして、サービス事業者の方々は一般の利用者に加え、そうしたDNS運用者にとっても安心して使え、**共に高め合っていける、優れたマネージドサービス**を提供してほしい

それが、DNSと31年関わってきた私の願いです

最後までご視聴いただき
ありがとうございました！

<https://jprs.jp/tech/>

@JPRS_official　　JPRSofficial