サブドメインテイクオーバーの概要とその防止策

2021年2月5日

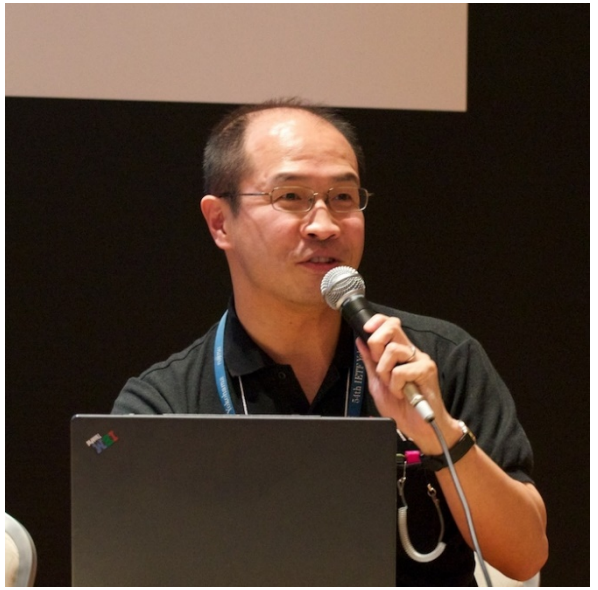
第1回フィッシング対策勉強会

株式会社日本レジストリサービス（JPRS）

森下 泰宏

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
  - 主な業務内容：ドメイン名・DNSに関する技術広報活動全般



＜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、運用に従事。
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及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）。

JPRSの概要

株式会社 日本レジストリサービス

JaPan Registry Services

■主な役割

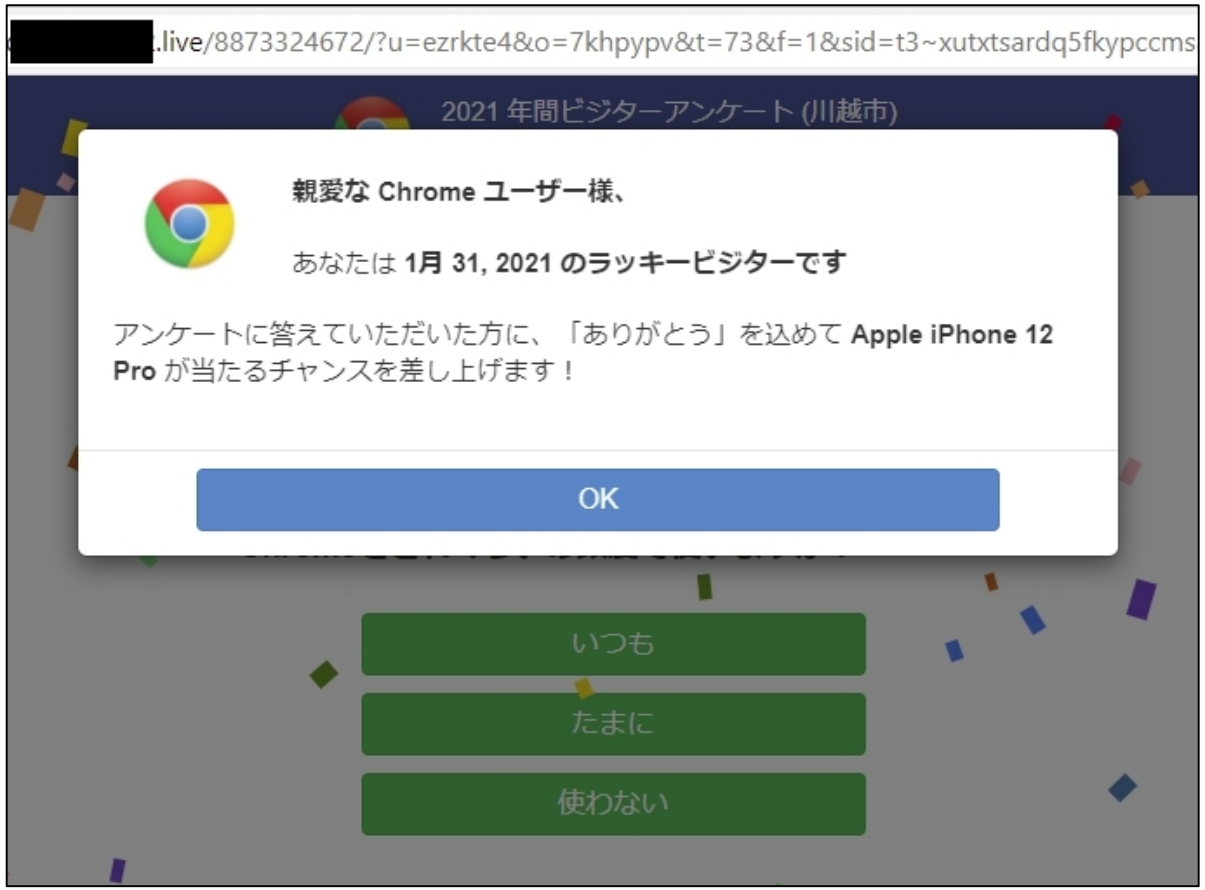
- JPドメイン名（.jp）の登録管理
- JP DNSの運用、 Mルートサーバーの共同運用
- インターネットのポリシー策定や技術の標準化など、国際活動・研究開発への貢献

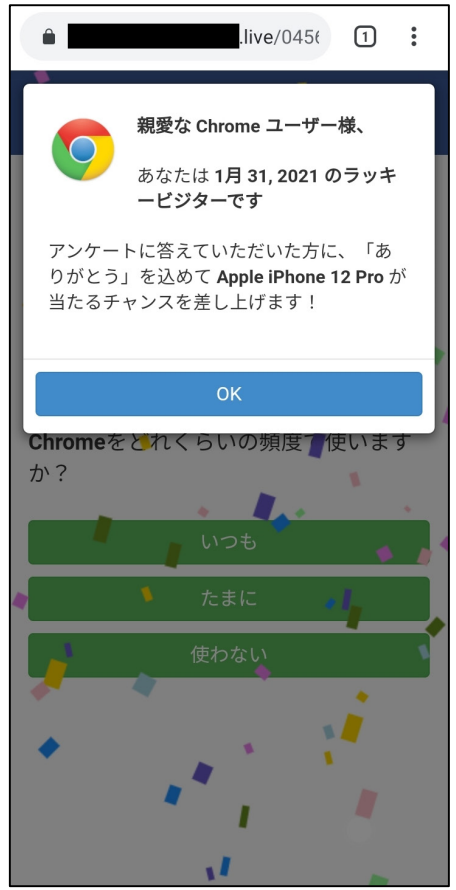
本日の内容

- DNSの運用ミスに付け込み、使い終わったサブドメインを標的とする「**サブドメインテイクオーバー**」の概要と防止策についてお話しします
- **講演20分+質疑応答10分**を予定しています

iPhoneが当たった？

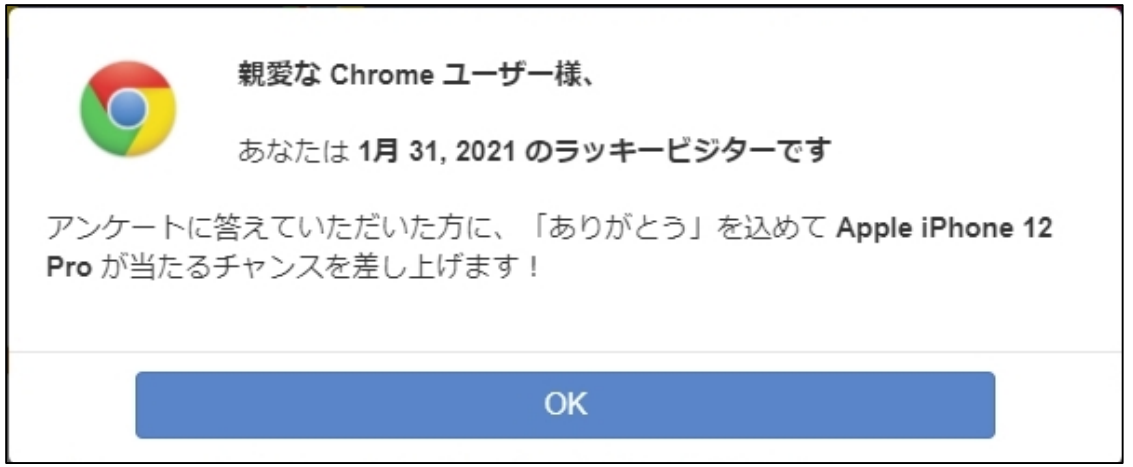
- 検索した際、**こんな画面**が表示されたことはありませんか？





これは**詐欺**です！

- **検索結果を開いた際**に「**iPhoneが当たるチャンスを差し上げます！**」という画面が表示され、**アンケート**に誘導
  - 個人情報・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



終了したWebサイトへのアクセスを奪取

- **終了したWebサイトへのアクセスを奪取**し、**詐欺サイト**や詐欺サイトに誘導するための**おとりサイト**を開設
  - アクセスの奪取には、さまざまな手法が使われている

アクセスを奪取する手法の例

- Webコンテンツの不正書き換え
- ドメイン名登録情報の不正書き換え
- DNSゾーン情報の不正変更
- DNSキャッシュポイズニング
- 利用者側機器のDNS設定の不正変更（例：DNS Changer）
- ドロップキャッチ
- **サブドメインテイクオーバー**

サブドメインテイクオーバーとは？

- **DNSの運用ミス**に付け込む攻撃手法の一つ
- **使い終わったサブドメイン**が標的
  - 例：**campaign.example.jp**
    - example.jpの管理者が、期間限定のキャンペーンサイトとして設定
- 使い終わった後、**残ったままになっているDNS設定**を利用
- 攻撃手法そのものは**以前から存在**
  - CDNサービスの普及により、**事例が増加中**

サブドメインテイクオーバーの**被害状況**

- 国内外の**複数の組織**が被害に
  - 2020年7月までに、**100件以上の被害事例**を確認
  - **地方公共団体**や、**上場企業**のドメイン名も含まれている
- 被害事例の報告は、**現在も続いている**
- **詐欺サイトへの誘導以外の不正行為**にも使われている
  - 本物のコンテンツをコピーし、リンクをアフィリエイト付きのものに差し替えた**偽サイトの作成**など

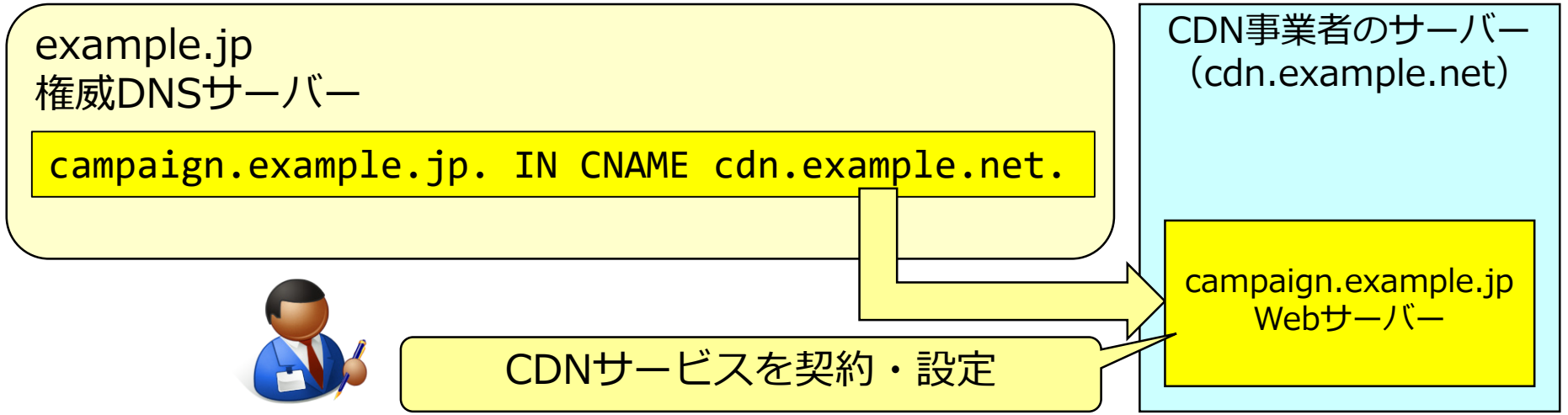
サブドメインテイクオーバーが発生する流れ（1/3）

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

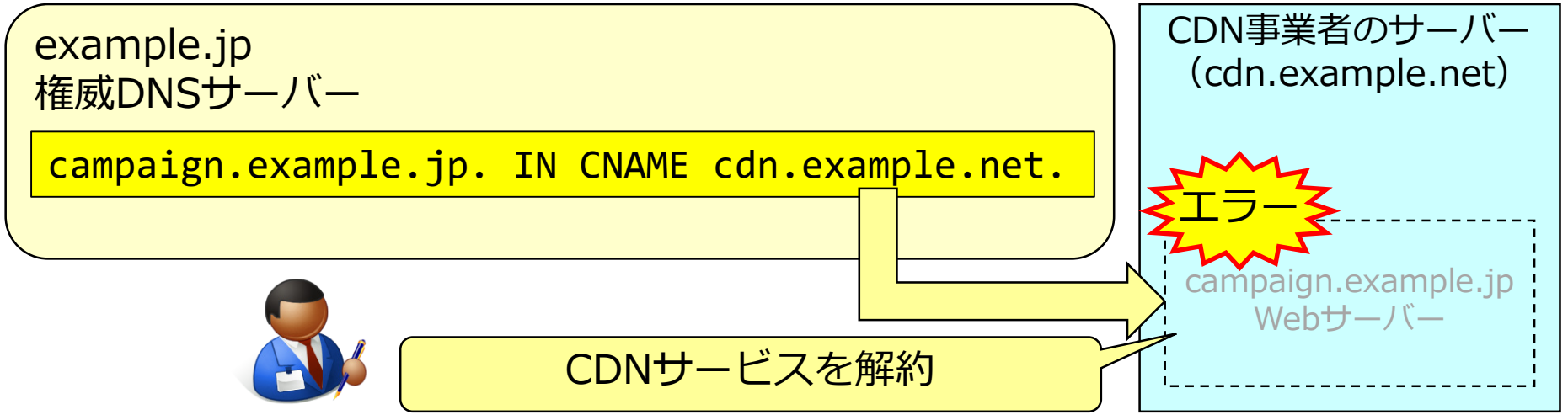
– **自分のドメイン名のサブドメイン**で、Webサイトを公開



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**

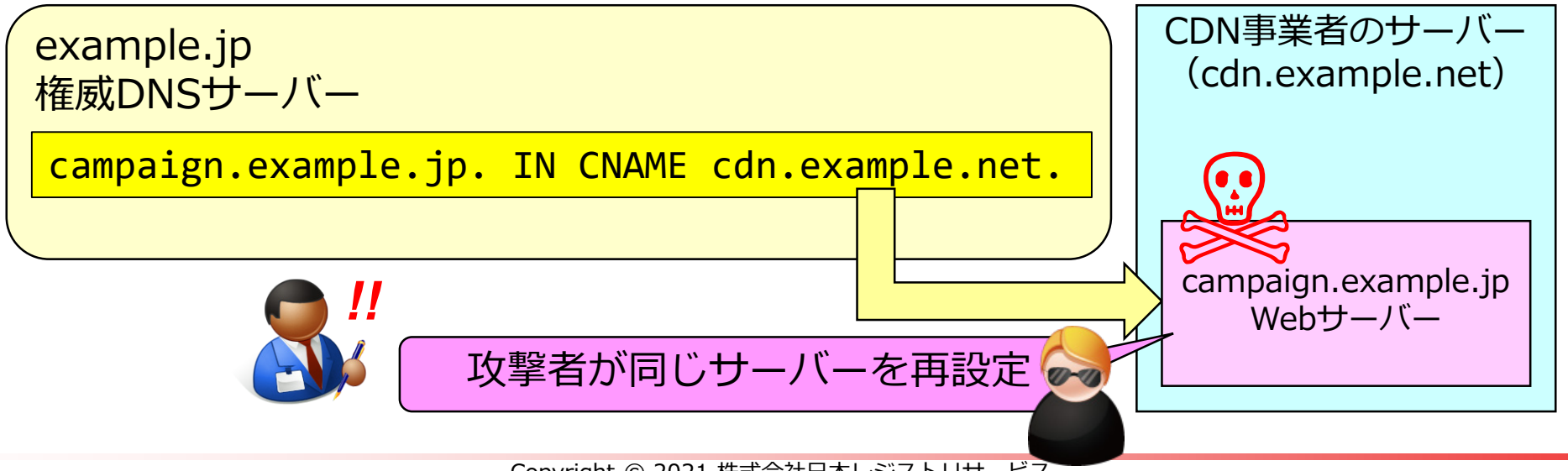
- **事業者側の設定を削除**、Webサイトにアクセスできない状態に
- 設定したCNAMEレコードは**残ったまま**
  - 削除の必要があることを認識していない or 削除を忘れている



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、**不適切なコンテンツを公開**



サブドメインテイクオーバーを用いた**SEOポイズニング**

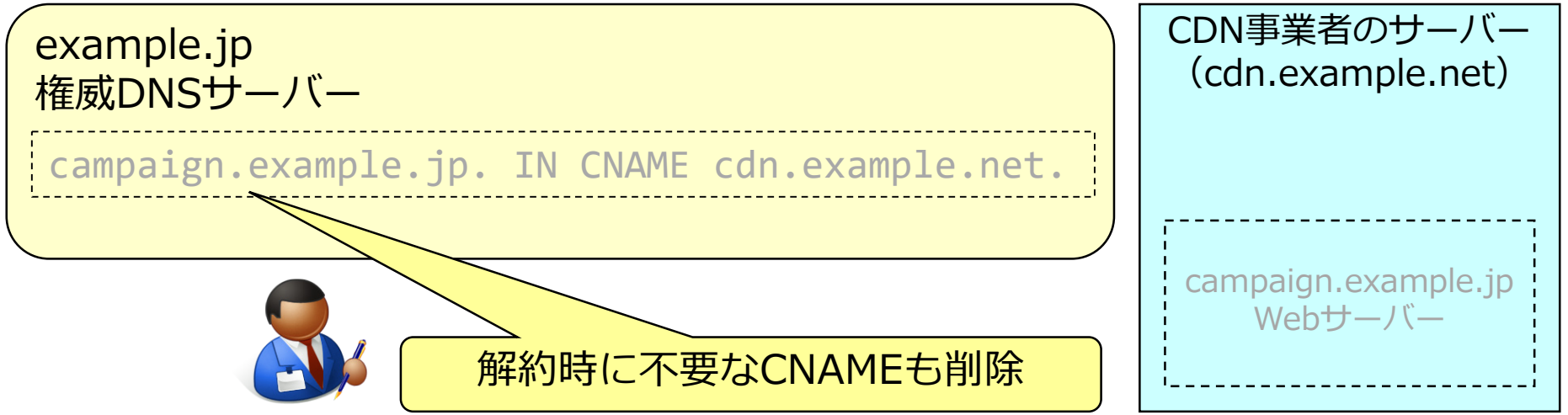
- iPhone当選詐欺では、**著名企業・自治体**などのサブドメインに、詐欺サイトに誘導するための**おとりサイト**を作成
- 著名なドメイン名や政府関係のドメイン名のサブドメインを使うことで、**検索で上位に表示される**ことを期待していると考えられる
- **SEOポイズニング**と呼ばれる手口の一つ

攻撃者が攻撃対象を見つける方法

- サブドメインテイクオーバー可能な状態は、**外部からのDNS検索**で発見可能
  - CNAMEの参照先に、**Webサイトの実体が存在しない**状態
- 利用可能なツールがインターネット上で公開
  - **総当たり検索**を高速に実行、サブドメインテイクオーバー可能な状態のドメイン名を発見

サブドメインテイクオーバーの防止策①

- 利用終了時に、**利用開始時に設定したDNS設定を削除**する
  - **CNAMEレコード・A/AAAAレコード**を削除



サブドメインテイクオーバーの防止策②

- **テイクオーバー可能な設定が残っていないかチェック**する
  - 例：Microsoft Azureでは、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テイクオーバー可能なDNS設定がないかを利用者が確認するための**チェックツール**を公開

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>

サブドメインテイクオーバーの防止策③

- **サブドメインテイクオーバーされにくいサービス**を使う
  - 例：Amazon CloudFrontにおける対策
    - 生成されるドメイン名（CNAME参照先）の**ランダム化**

代替ドメイン名 (CNAME) を追加してカスタム URL を使用する - Amazon CloudFront
<https://docs.aws.amazon.com/ja_jp/AmazonCloudFront/latest/DeveloperGuide/CNAMEs.html>

    - 利用者が設定するドメイン名の**管理権限の確認（サーバー証明書**の提出）

Amazon CloudFront がディストリビューションに代替ドメイン名を追加する際のセキュリティを強化
<https://aws.amazon.com/jp/about-aws/whats-new/2019/04/amazon-cloudfront-enhances-the-security-for-adding-alternate-domain-names-to-a-distribution/>

本日のまとめ（概要と防止策）

- サブドメインテイクオーバーの**概要**
  - **DNSの運用ミス**に付け込み、**使い終わったサブドメイン**を攻撃
  - **残ったままになっているDNS設定**を利用
  - CDNサービスの普及により、**被害事例が増加中**
  - **検索で上位に表示される**ことを利用（**SEOポイズニング**）
- サブドメインテイクオーバーの**防止策**
  1. 利用終了時に、利用開始時に設定した**DNS設定を削除**する
  2. テイクオーバー可能なDNS設定が**残っていないかチェック**する
  3. サブドメインテイクオーバー**されにくいサービス**を使う

今すぐチェックを！

おわりに：JPRSの技術情報発信

- ドメイン名・DNS・サーバー証明書に関する**技術情報**を発信中！
- JPRS **DNS関連技術情報**

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

  QRコードはこちら
- JPRS**用語辞典**

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

  QRコードはこちら
- SNS**公式アカウント**

@JPRS_official

JPRSofficial

Q & A