最近勉強したこと

2025/1/29

先週 JPRS がある記事を発表した

■サービス終了後に残っているDNS設定を利用したサブドメインの乗っ取りについて

株式会社日本レジストリサービス（JPRS）
初版作成 2025/01/21（Tue）

▼概要

レンタルサーバーやCDN（Content Delivery Network）など、事業者のサービスを利用して自身のドメイン名のサブドメイン（例：sub.example.co.jp）でWebサイトを公開する場合、事業者のサーバーを参照するDNS設定を自身のドメイン名の権威DNSサーバーに追加することで、Webサイトを提供できる状態になります。

しかし、Webサイトの公開を終了する際に公開時に追加したDNS設定を削除・変更せず、事業者のサーバーを参照したままになっている場合、残っている

https://jprs.jp/tech/security/2025-01-21-danglingrecords.html

記事の要約

- ダングリングレコードがあると、サブドメインテイクオーバーの被害に遭う可能性がある
- これらの被害に遭わないためにも、不要になったレコードは忘れずに削除することが重要

いくつか知らない単語があったので調べてみた

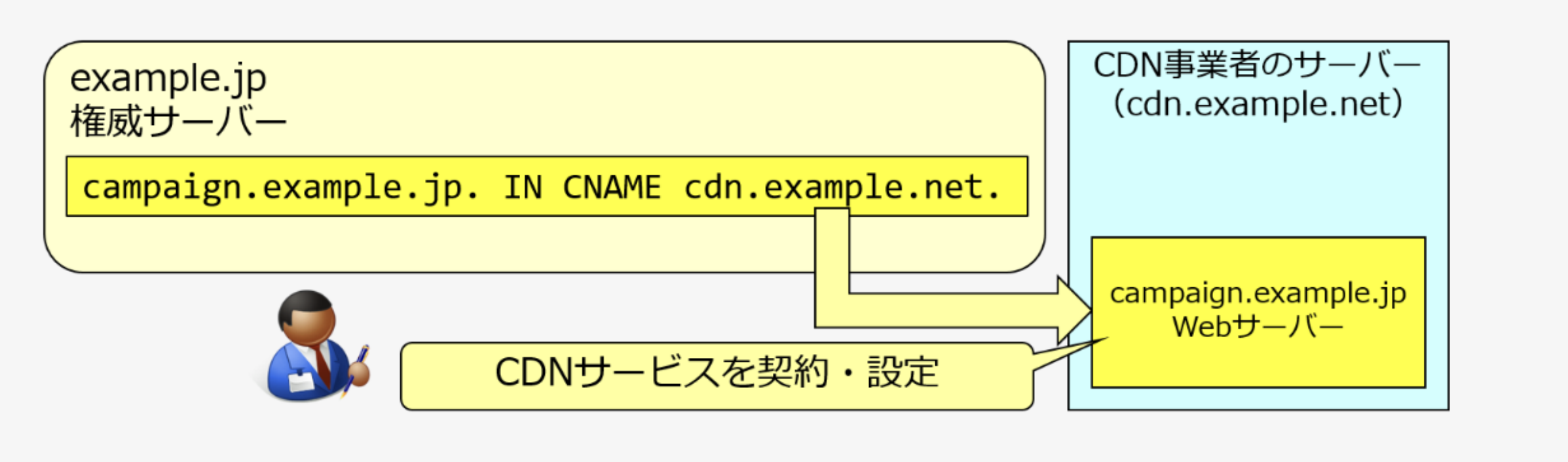
- ダングリングレコードがあると、サブドメインテイクオーバーの被害に遭う可能性がある
- これらの被害に遭わないためにも、不要になったレコードは忘れずに削除することが重要

dangling records（ダングリングレコード）

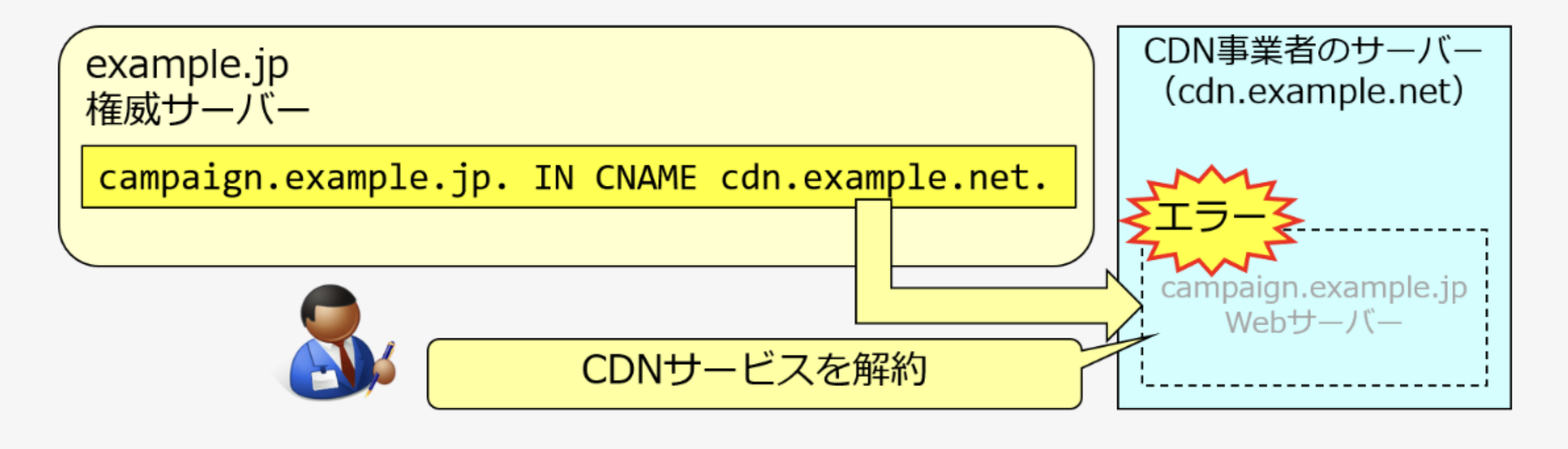
- 指定された名前の実体が無効になっている DNS レコード
- e.g. CNAME レコードの指定先に CDN が存在しない, A レコードの指定先に Web サーバーが存在しない

サブドメインテイクオーバー

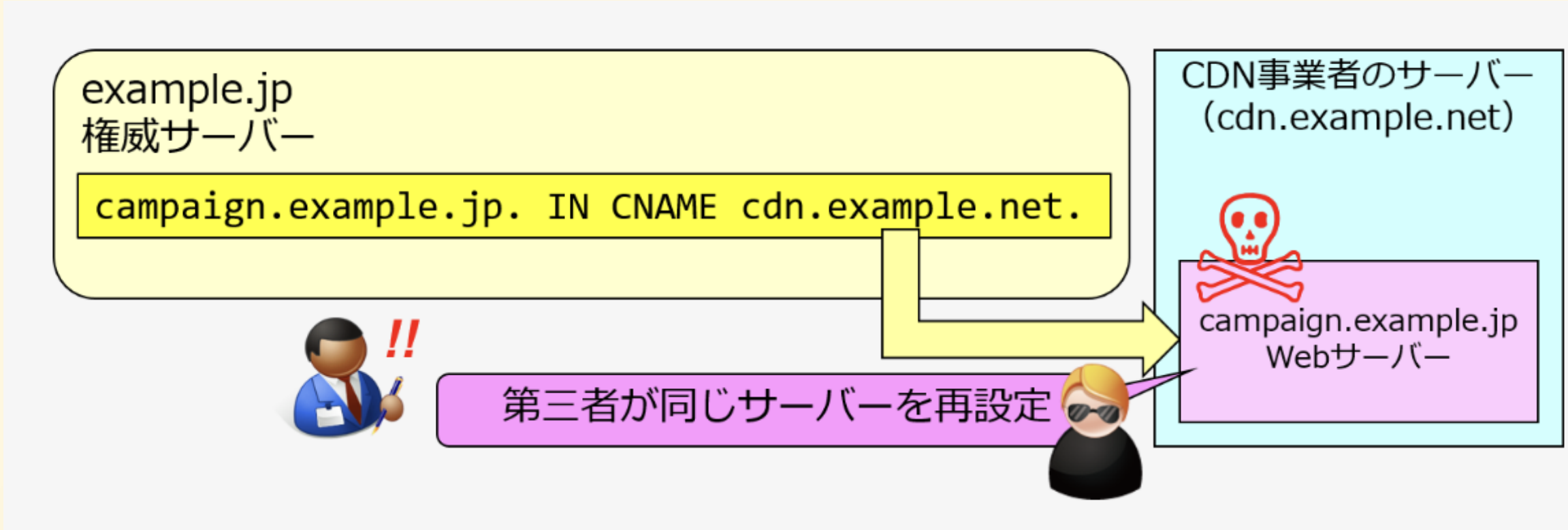
- ドメインの管理権限を持たない第三者が、そのサブドメインの乗っ取りを図る攻撃手法



campaign.example.jp にリクエストが来たら cdn.example.net の CDN にリクエストを流すサービス

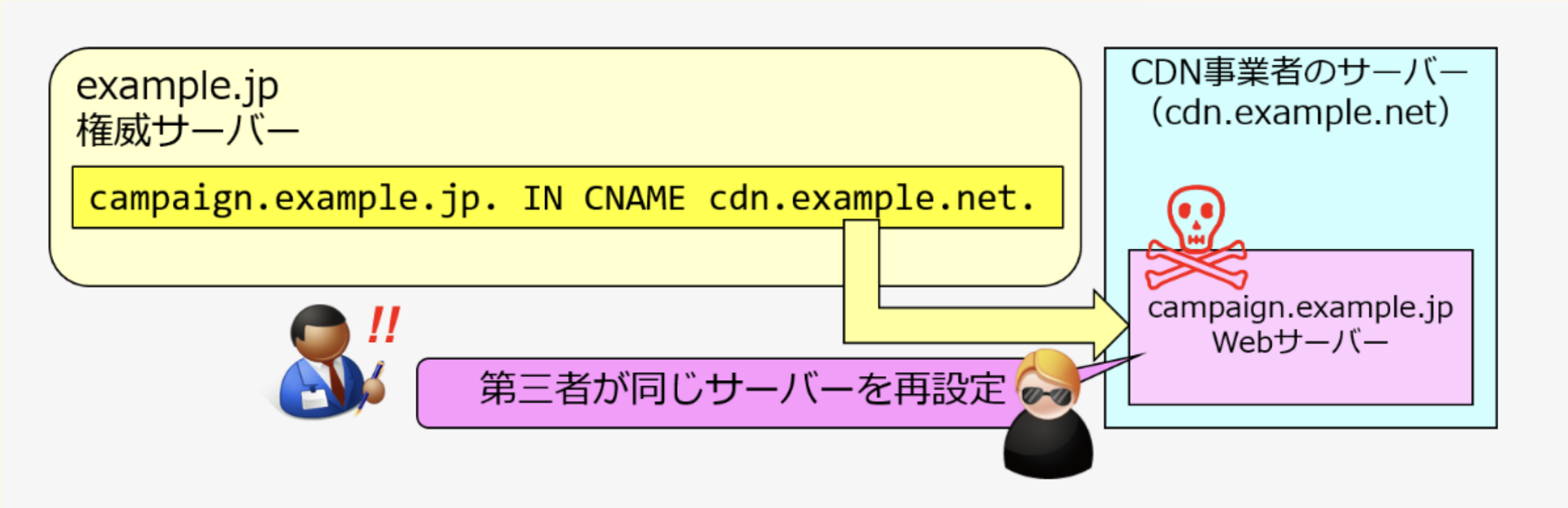

example.jp
権威サーバー
campaign.example.jp. IN CNAME cdn.example.net.
CDN事業者のサーバー
(cdn.example.net)
エラー
campaign.example.jp
Webサーバー
CDNサービスを解約

CDN サービスを解約



第三者が CDN を契約して cdn.example.net のサーバー設定を追加

campaign.example.jp が悪意のあるサイトに成り代わってしまう



乗っ取られないためには不要になった DNS レコードは削除しておくことが重要

まとめ

- **dangling records（ダングリングレコード）**
  - 指定された名前の実体が無効になっているリソースレコード
- **サブドメインテイクオーバー**
  - ドメインの管理権限を持たない第三者が、そのサブドメインの乗っ取りを図る攻撃手法
- **不要になったレコードは忘れずに消す**のが大切