終わったWebサイトのDNS設定、そのままになっていませんか？

～サブドメインテイクオーバー・NSテイクオーバーの概要と対策～

2025年6月11～13日

Interop Tokyo 2025

本セミナーの内容

- DNS設定がそのままになっていると…
- サブドメインテイクオーバー・
  NSテイクオーバーの概要
- サブドメインテイクオーバー・
  NSテイクオーバーの対策
- DNS運用者・責任者のみなさまへ

NHKニュース（2025年1月）

- ドメイン名の不正利用に関する複数の事例が報道

省庁ウェブサイトのドメイン管理不十分 5省庁に 厚労省なども

2025年1月10日 5時40分

総務省の一部ウェブサイトにセキュリティー上の不備があった問題で、各省庁が確認したところ、厚生労働省や文部科学省など少なくとも5つの中央省庁のウェブサイトでも、ドメインの管理について、同様の不備があったことがわかりました。監督するデジタル庁によると、すでに修正を行っているというこ

総務省などの一部のウェブサイトについて、12月に外部から、セキュリティー対策が不十分で第三者が不正利用できる状態になっていると指摘があり、総務省は、ドメインの管理に不備があったことを認めて、修正を行いました。

第三者が不正利用

引用元：<https://www3.nhk.or.jp/news/html/20250110/k10014689351000.html>

国交省 過去に使ったドメイン オンラインカジノ広告に一時流用

2025年1月10日 17時16分

過去に使ったドメイン

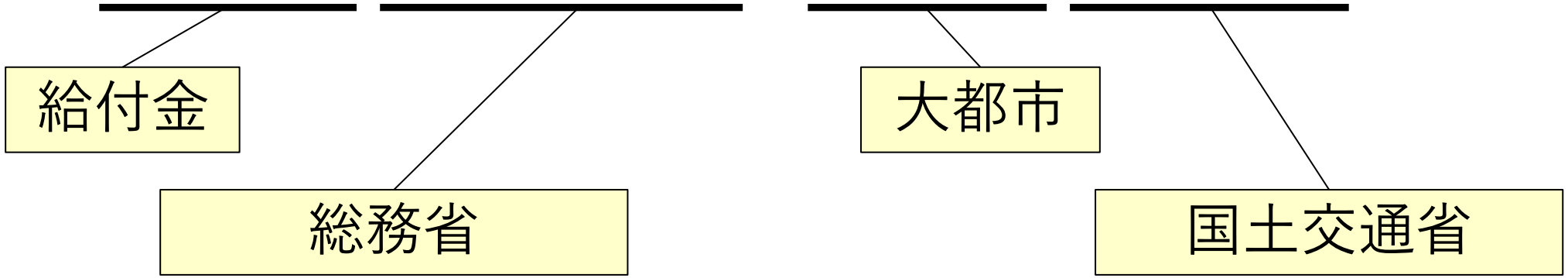
総務省など複数の中央省庁の一部ウェブサイトに、セキュリティー上の不備があった問題で、国土交通省が過去に使ったウェブサイトのドメインがタイのオンラインカジノにつながる広告サイトに一時流用されていたことがわかりました。外部からの指摘で、現在は修正されていますが、専門家は、「信頼性が高い政府機関のドメインが、不正なサイトに使われたことは非常に大きな問題だ」としています。

総務省や厚生労働省など5つの中央省庁では、一部のウェブサイトがセキュリティー対策が不十分で第三者が不正利用できる状態になっていたことが外部からの指摘で明らかになりました。

引用元：<https://www3.nhk.or.jp/news/html/20250110/k10014689801000.html>

何が起こったのか？

- 過去に使ったドメイン名を第三者に不正利用された
- 組織のドメイン名のサブドメインが主な標的に
  - 例：kyufukin.soumu.go.jp、daitoshi.mlit.go.jpなど



標的となったドメイン名の例

- いずれも、期間限定のWebサイトで使われていた

https://kyufukin.soumu.go.jp/

- 特別定額給付金ポータルサイト（2020年）
  （新型コロナウイルス感染症緊急経済対策）

https://daitoshi.mlit.go.jp/

- 大都市交通センサス公式Webサイト（2010、2015、2021年）
  （大量公共交通機関の利用実態調査）

使い終わったドメイン名を使われるパターン

- 大きく2種類に分類される

今回はこれに注目する

① ドメイン名を再登録する

- 更新されなかったドメイン名は有効期限満了後、廃止される
- そのドメイン名を再登録し、同じ名前でWebサイトを復活させる
  - 登録可能になる瞬間を狙った再登録を、ドロップキャッチと呼ぶ

② DNS設定の案内先を勝手に使う

- Webサイトの運用終了後にそのままになっているDNS設定の案内先を勝手に使って、同じ名前でWebサイトを復活させる

今回の事例はいずれも、②によるもの

DNS設定の案内先を勝手に使う

- 残っている看板（DNS設定）を利用し、案内先の跡地を別のことに使う（跡地を無断で使う ＝ テイクオーバー）

以降の内容について

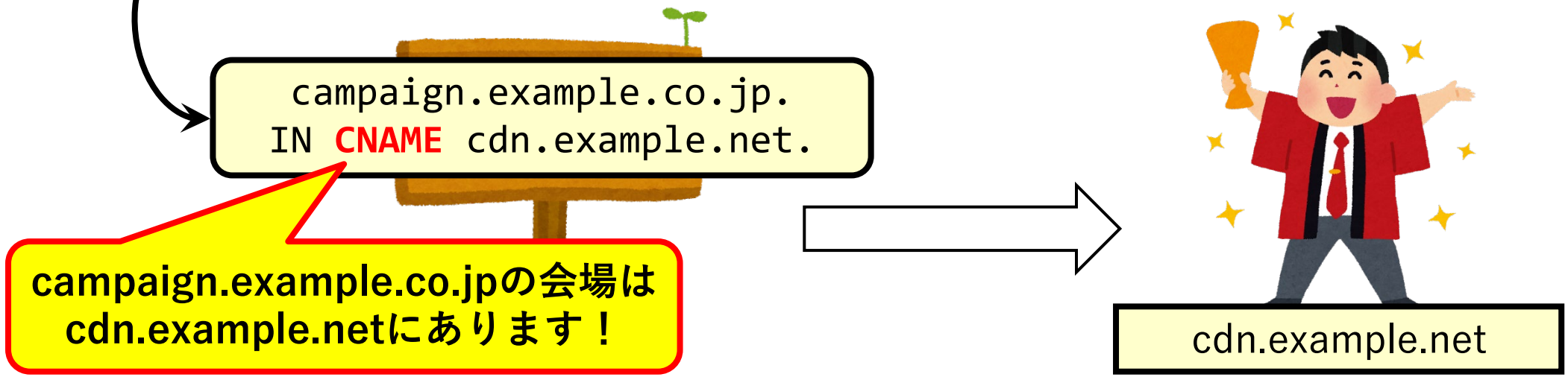
- 以降ではテイクオーバーの代表的な手法である、サブドメインテイクオーバーとNSテイクオーバーについて解説する
  - サブドメインテイクオーバーを中心に解説するが、手法の概要・対策は共通

サブドメインテイクオーバー・NSテイクオーバーの概要

「案内の看板」に使われるDNS設定

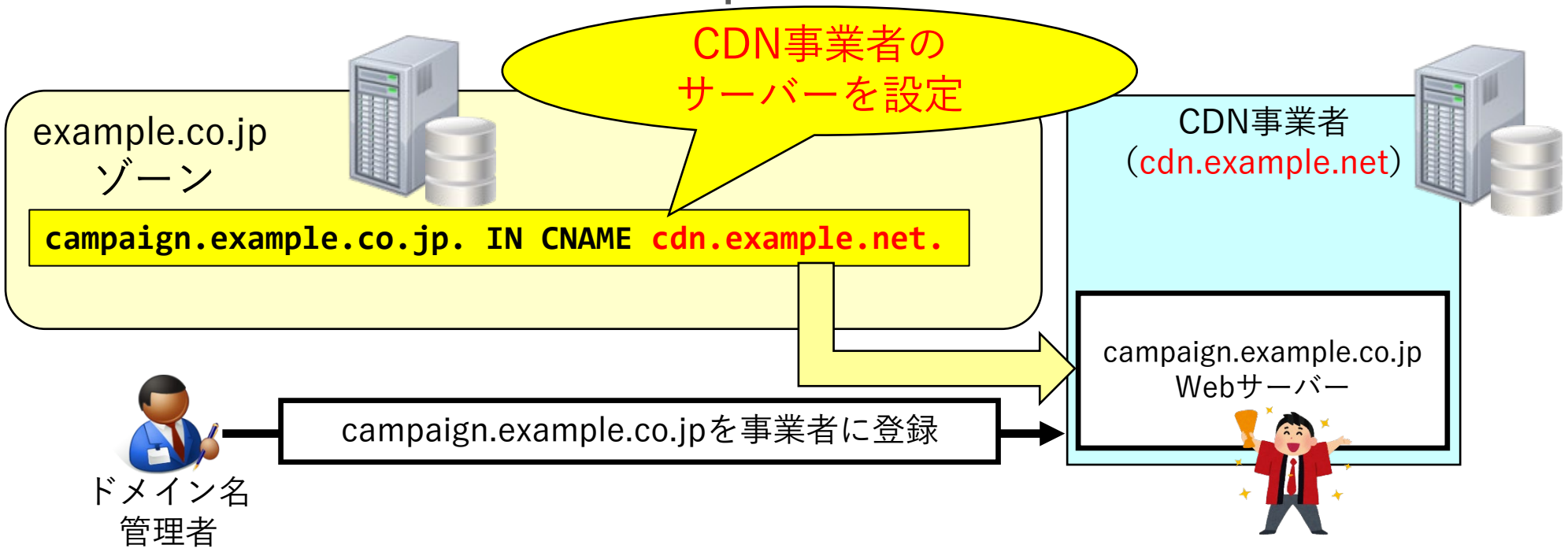
- CNAMEレコードやNSレコードが使われる
  - CNAMEレコードの設定例：

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



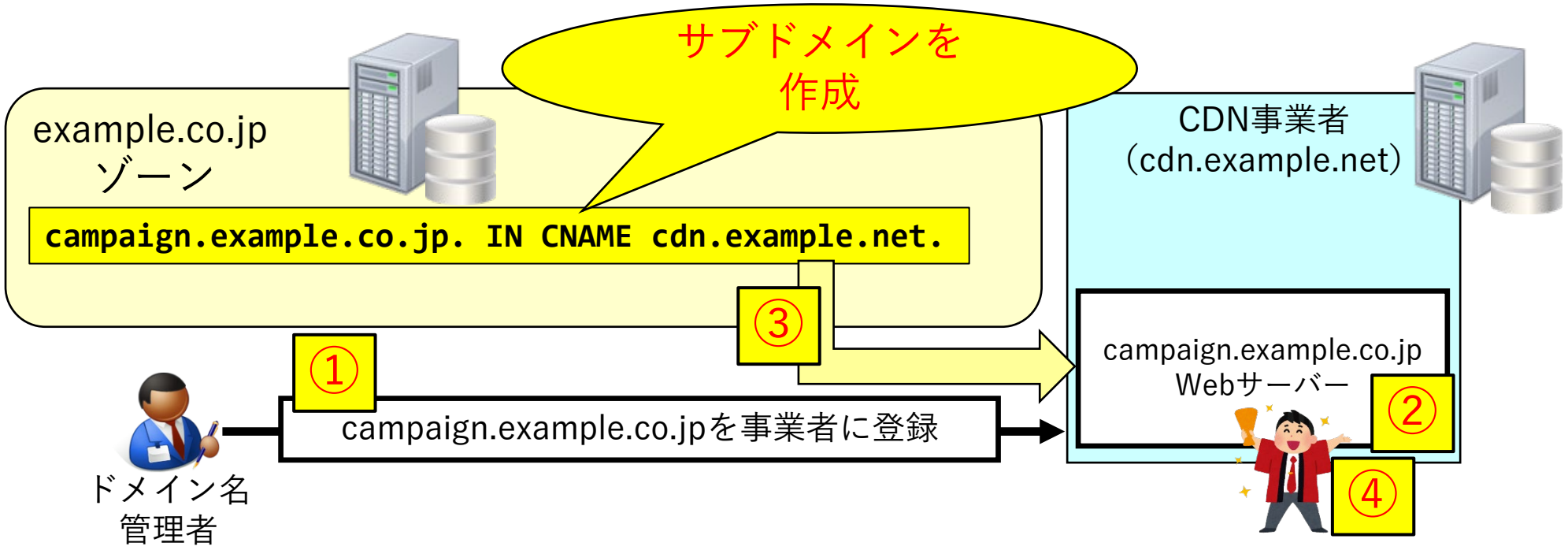
CNAMEレコードの設定例

- サービスを提供するCDN事業者のサーバーを設定
  - 意味：「campaign.example.co.jpのWebサーバーは、CDN事業者のcdn.example.netサーバーの中に入っています」



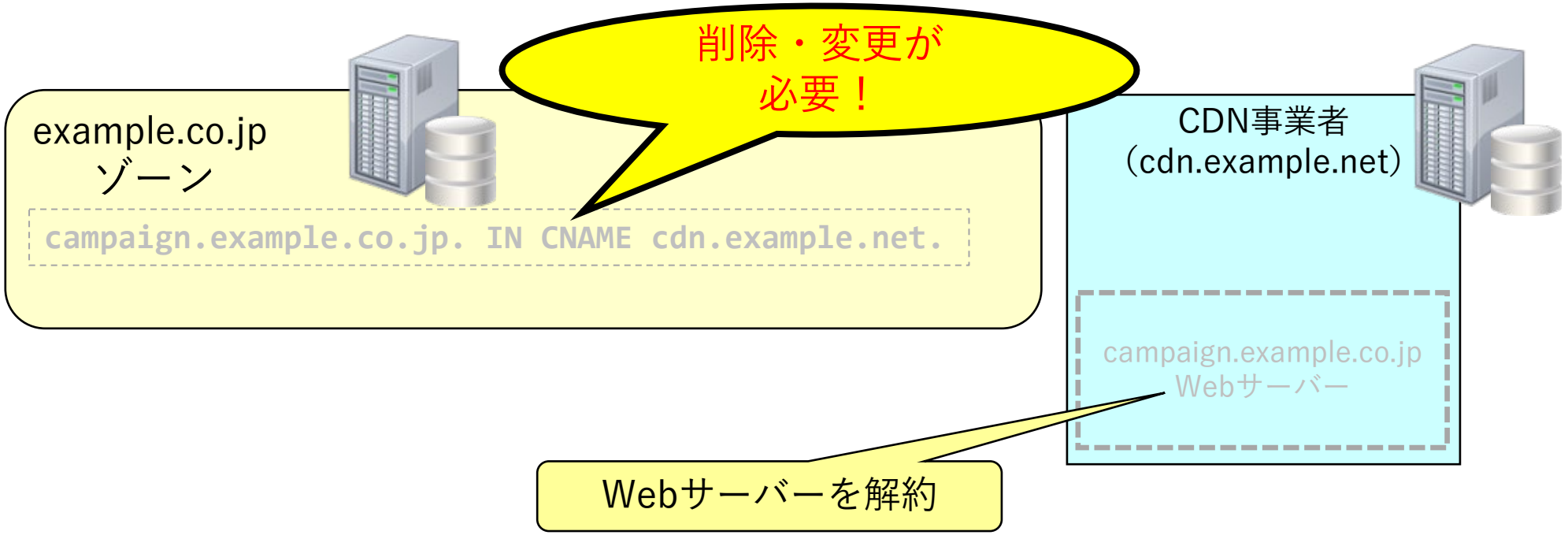
CNAMEを用いたWebサーバーの設定手順

① CDN事業者と契約し、campaign.example.co.jpを設定する権限を取得する
② cdn.example.netにcampaign.example.co.jpのWebサーバーを作成する
③ CNAMEレコードを設定し、example.co.jpのサブドメインを作成する
④ WebサーバーにWebコンテンツを設定する



Webサイト終了時はDNS設定の削除が必要

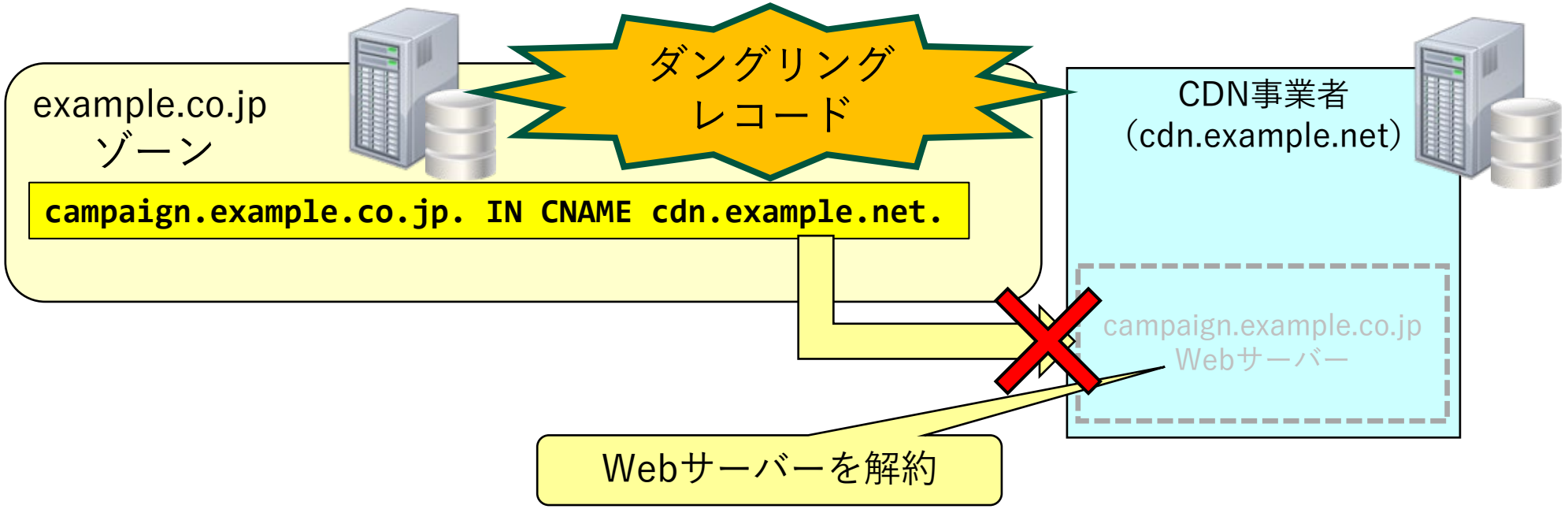
- Webサイトを終了した場合、ドメイン名の管理者は設定した CNAME・NSレコードを削除・変更する必要がある
- もし、DNS設定が残っていると…



ダングリングレコード

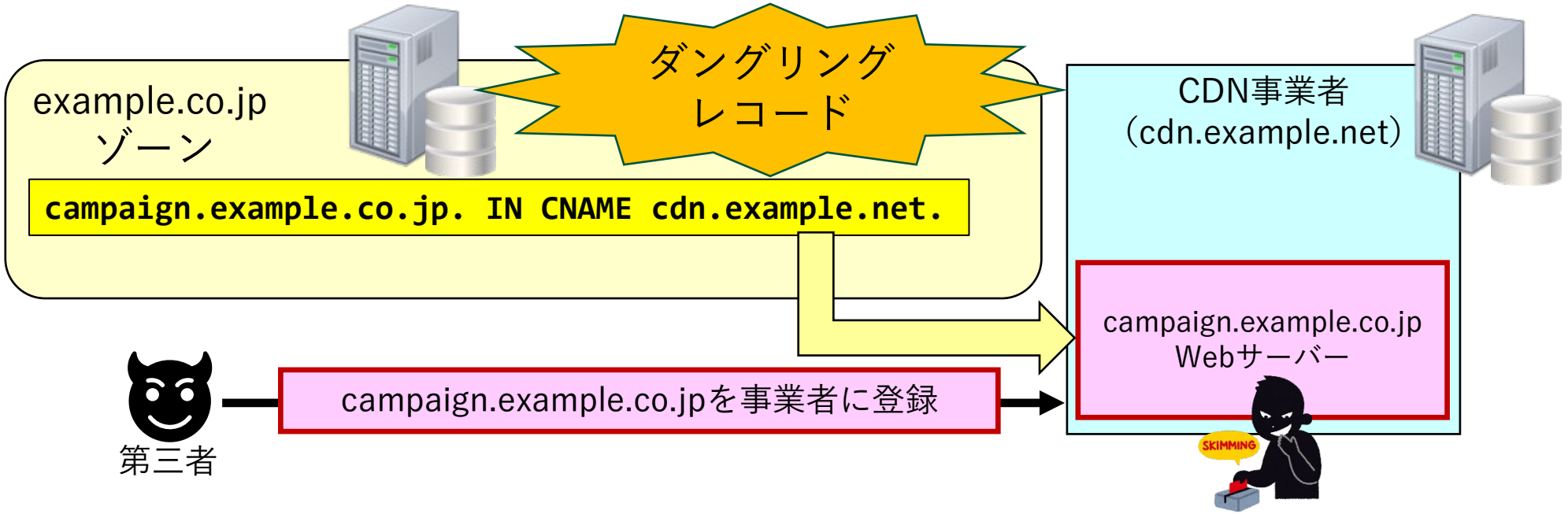
※ダングリング（dangling）：宙ぶらりんの

- DNS設定が残っていると、ダングリングレコードになる
  - ダングリングレコードはサブドメインテイクオーバー・NSテイクオーバーされる潜在的なリスクとなる



サブドメインテイクオーバー

- ダングリングレコードの参照先に同じWebサーバーを作成し、不適切なWebコンテンツを設定することで、意図しないWebコンテンツの公開を図る手法



サブドメインテイクオーバーの手順

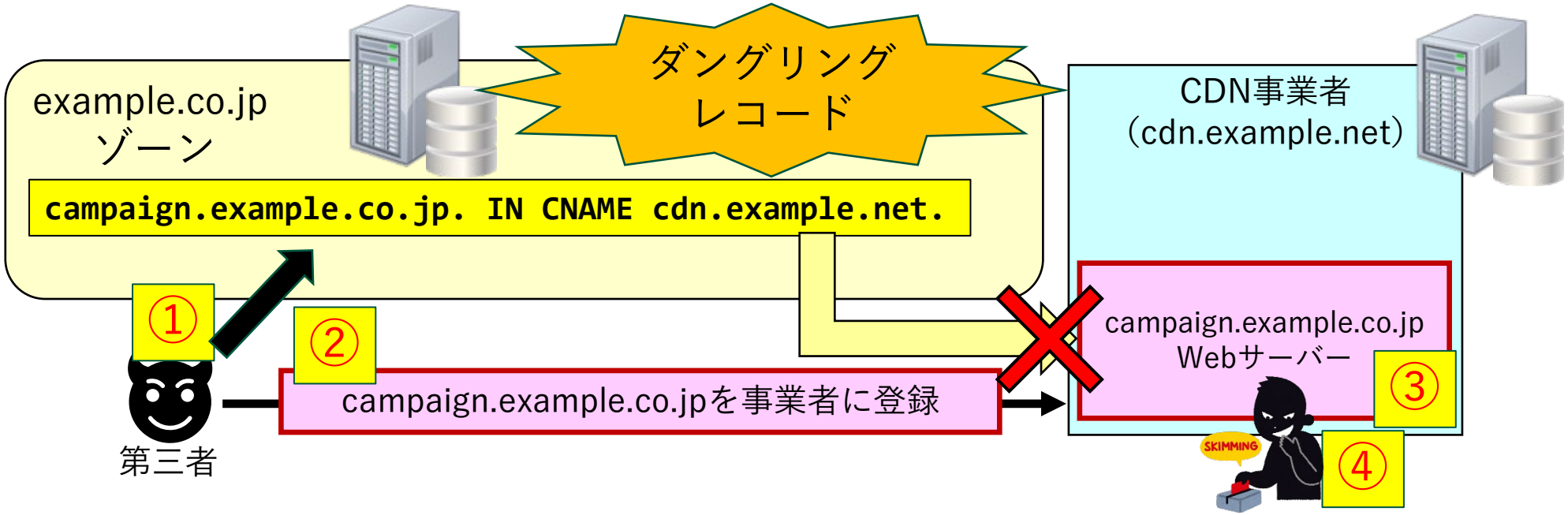
① 攻撃可能なダングリングレコードを見つける

どう見つけるのか？

② campaign.example.co.jpの権限を取得するため、参照先のCDN事業者と契約する

③ 参照先のサーバーにcampaign.example.co.jpのWebサーバーを作成する

④ Webサーバーに不適切なWebコンテンツを設定する



標的を見つける方法（1/3）

- 外部からのDNSスキャニングで検出する
  - 高速なスキャニングツールがGitHub等で公開
    - DNS運用者には防御ツールに、攻撃者には攻撃ツールになる
- 稼働中のWebサイトのDNS設定を調べて候補を選ぶ
  - WebサイトのDNS設定は公開情報
    - 稼働中に、終了後にサブドメインテイクオーバーできる可能性があるドメイン名の「当たりをつける」ことができる

標的を見つける方法（2/3）

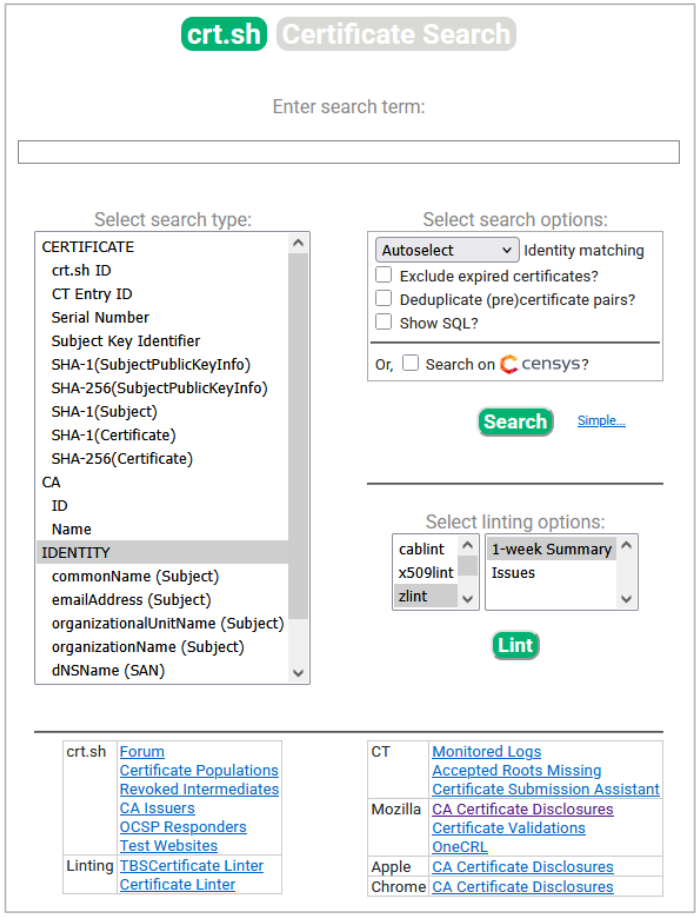
- サーバー証明書のCTログを利用する
  - 証明書の誤発行・不正発行を検知する仕組み
  - 発行されたすべてのサーバー証明書は Certificate Searchサイトで検索可能
- 出力例（kyufukin.soumu.go.jp）

Certificates

crt.sh ID	Logged At ⇧	Not Before	Not After	Common Name	Matching Identities	
16195150621	2024-12-21	2024-12-21	2025-03-21	kyufukin.soumu.go.jp	kyufukin.soumu.go.jp	C=US, O=
15845762076	2024-12-21	2024-12-21	2025-03-21	kyufukin.soumu.go.jp	kyufukin.soumu.go.jp	C=US, O=
3637762760	2020-11-12	2020-11-10	2021-11-30	kyufukin.soumu.go.jp	kyufukin.soumu.go.jp www.kyufukin.soumu.go.jp	C=JP, O=
3627700099	2020-11-10	2020-11-10	2021-11-30	kyufukin.soumu.go.jp	kyufukin.soumu.go.jp www.kyufukin.soumu.go.jp	C=JP, O=
2764416887	2020-05-04	2020-04-28	2021-04-28	kyufukin.soumu.go.jp	kyufukin.soumu.go.jp	C=US, O=
2740465286	2020-04-28	2020-04-28	2021-04-28	kyufukin.soumu.go.jp	kyufukin.soumu.go.jp	C=US, O=

第三者が発行要求した証明書

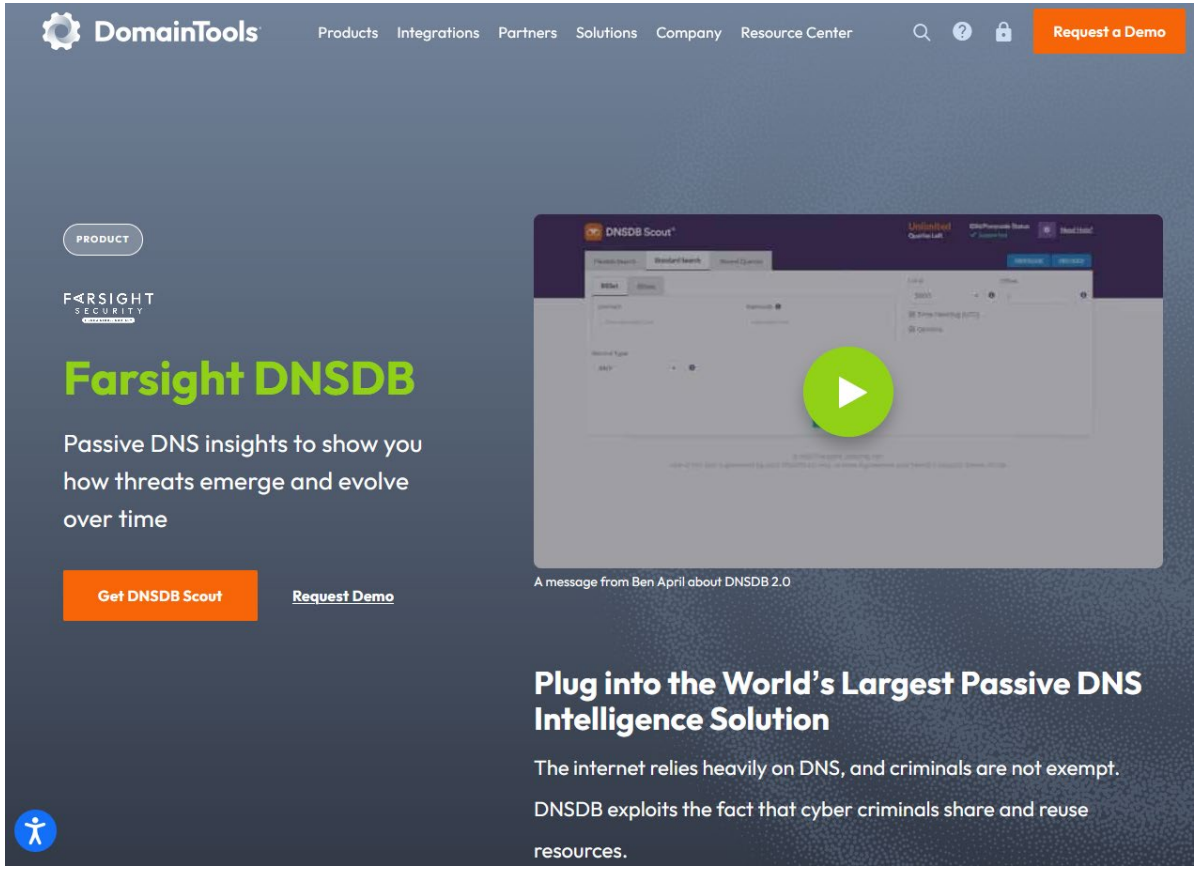
ドメイン名管理者が発行要求した証明書



<https://crt.sh/?a=1>

標的を見つける方法（3/3）

- Passive DNSを利用する
  - DNS応答を収集・保存し、ドメイン名の利用状況やセキュリティ上の脅威の分析に役立てる仕組み
  - Farsight DNSDBなど、複数の組織がサービスを提供



<https://www.domaintools.com/products/farsight-dnsdb/>

サブドメインテイクオーバー・NSテイクオーバーの対策

取り得る対策の種類

- DNS運用者における対策
- サービス事業者における対策

サブドメインテイクオーバー・NSテイクオーバーでは、
DNS運用者とサービス事業者の双方における対策が必要

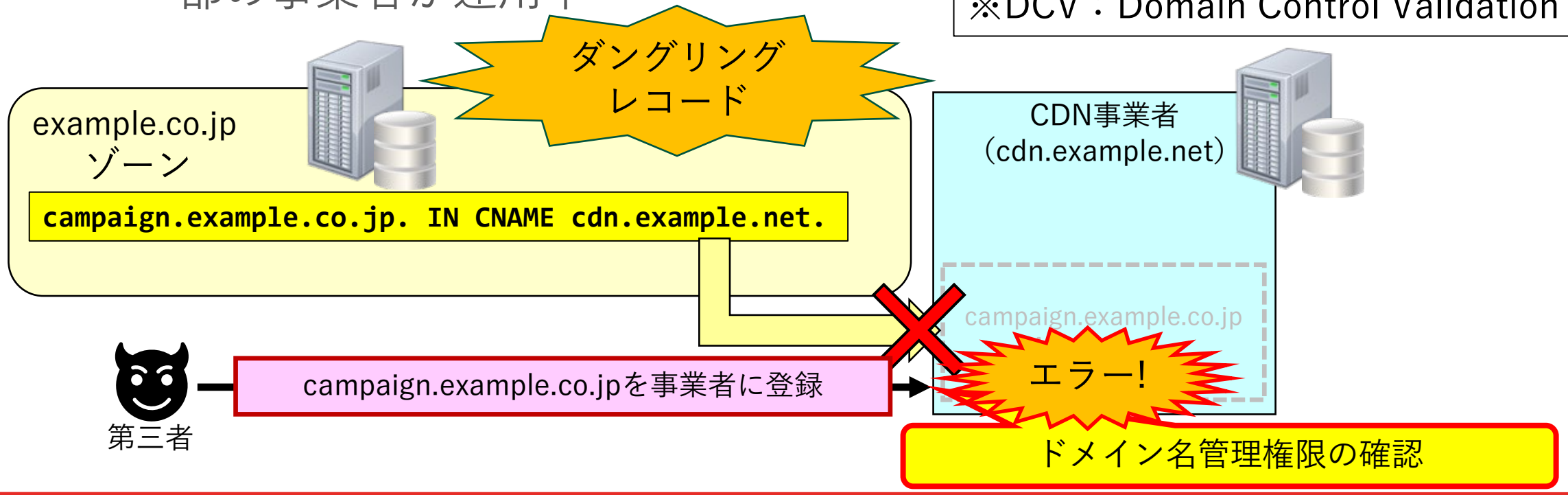
DNS運用者における対策

- Webサイト終了時のDNS設定の削除・変更
- DNSスキャニングツールによる定期的なチェック
  - ダングリングレコードの存在をチェックし、適切に削除・変更

サービス事業者における対策（1/3）

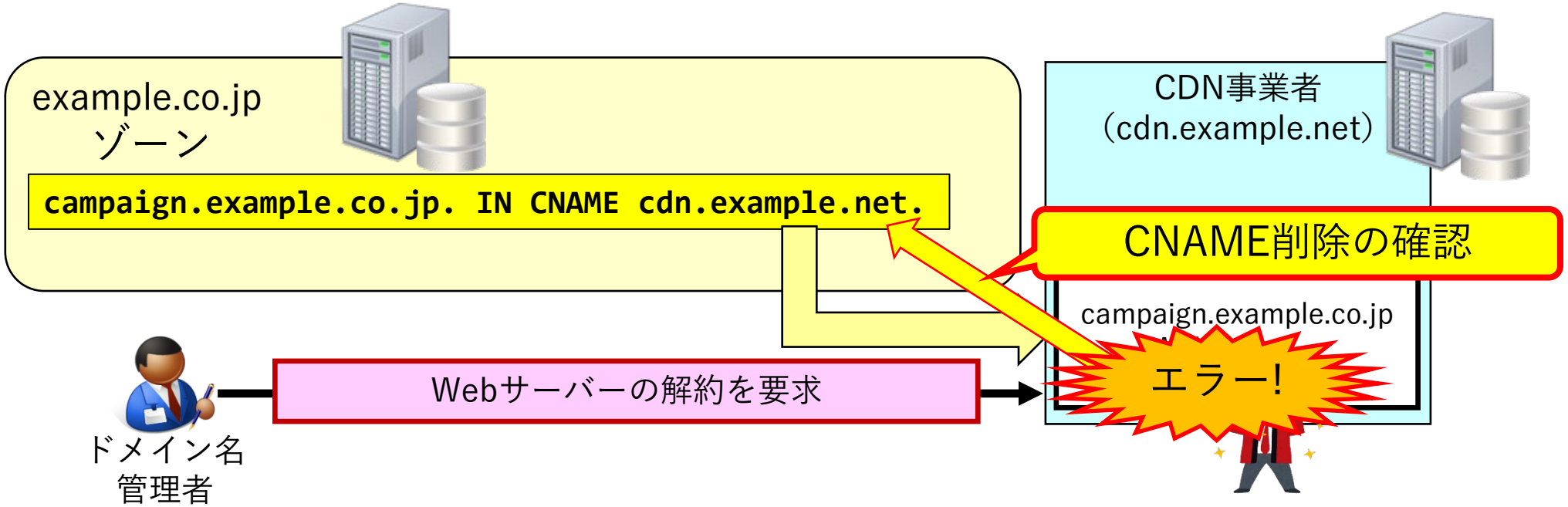
- サービス提供時のドメイン名管理権限の確認（DCV）
  - 権限を確認できなかった場合、サービス提供をエラーにする
    - 一部の事業者が運用中

※DCV：Domain Control Validation



サービス事業者における対策（2/3）

- サービス解約時のDNS設定削除の確認
  - DNS設定が残っていた場合、解約をエラーにする
    - 一部の事業者が運用中



サービス事業者における対策（3/3）

- テイクオーバーが困難なサービスの構築・運用
  - 例：CNAME・NSレコードの参照先のドメイン名として契約ごとに異なるランダムなラベルを生成・使用する
    - 一部の事業者が運用中

```
www.example.jp. IN CNAME d173o0niwo96y1.example.net.
```

CNAMEレコードの設定例（ドメイン名は例示用に変更済み）

```
example.or.jp.   IN NS ns019-e5l0ajvig3adn0c3.e.example.info.
                 IN NS ns019-e5l0ajvig3adn0c3.e.example.net.
                 IN NS ns019-e5l0ajvig3adn0c3.e.example.jp.
```

NSレコードの設定例（ドメイン名は例示用に変更済み）

DNS運用者・責任者のみなさまへ

本セミナーのまとめ

- サブドメインテイクオーバー・NSテイクオーバーの対策には、ドメイン名・DNSの適切な管理が必要です

ドメイン名の再登録（ドロップキャッチ）の対策と同様です

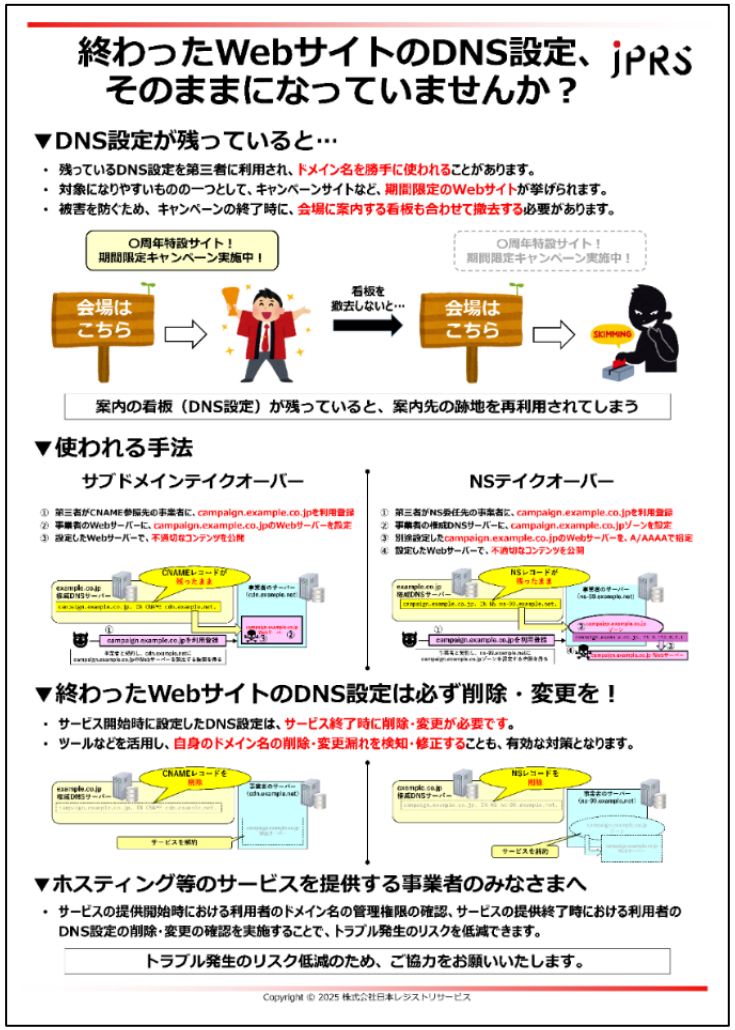
- DNS運用者における対策に加え、サービスを提供する事業者における対策も重要です

レンタルサーバーサービス・CDNサービス・DNSサービス等を提供する、事業者における対応も必要になります

PDFを配布中！

- PDFはこちらから入手できます

<https://jprs.jp/tech/security/2025-01-21-danglingrecords.pdf>



終わったWebサイトのDNS設定、JPRS
そのままになっていませんか？

▼DNS設定が残っていると…

- 残っているDNS設定を第三者に利用され、ドメイン名を勝手に使われることがあります。
- 対象になりやすいものの一つとして、キャンペーンサイトなど、期間限定のWebサイトが挙げられます。
- 被害を防ぐため、キャンペーンの終了時に、会場に案内する看板も合わせて撤去する必要があります。

案内の看板（DNS設定）が残っていると、案内先の跡地を再利用されてしまう

▼使われる手法

サブドメインテイクオーバー

NSテイクオーバー

▼終わったWebサイトのDNS設定は必ず削除・変更を！

- サービス開始時に設定したDNS設定は、サービス終了時に削除・変更が必要です。
- ツールなどを活用し、自身のドメイン名の削除・変更漏れを検知・修正することも、有効な対策となります。

▼ホスティング等のサービスを提供する事業者のみなさまへ

- サービスの提供開始時における利用者のドメイン名の管理権限の確認、サービスの提供終了時における利用者のDNS設定の削除・変更の確認を実施することで、トラブル発生のリスクを低減できます。

トラブル発生のリスク低減のため、ご協力をお願いいたします。