2025年2月18日
第77回JPドメイン名諮問委員会
参考資料4

DNS関連技術情報のトップへ戻る

■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DNS設定がサブドメインの乗っ取りに利用され、意図しないWebサイトの設定、フィッシング、個人情報の窃取など、さまざまなサイバー攻撃に利用される可能性があります。

こうした状況の発生を防ぐため、Webサイトを公開する際に追加したDNS設定はWebサイトの公開を終了する際に、削除・変更する必要があります。

▼詳細

事業者のサービスを利用し、example.co.jpというドメイン名の管理者がcampaign.example.co.jpというドメイン名でキャンペーン用のWebサイトを設定する際に、example.co.jpの権威DNSサーバーに追加するDNS設定の例を、以下に示します。

・設定例1：CDN事業者のWebサーバーを参照するCNAMEレコードを設定

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

・設定例2：クラウド事業者の権威DNSサーバーを参照するNSレコードを設定

```
$ORIGIN example.co.jp.
campaign IN NS ns-11.example.com.
         IN NS ns-33.example.org.
         IN NS ns-55.example.net.
```

事業者のサービスを解約して当該Webサイトの公開を終了する場合、公開時に設定した、事業者のサーバーを参照するDNS設定を削除・変更する必要があります。設定が残ったままになっている場合、それらの設定はサービスの解約後、参照先のWebサーバーや権威DNSサーバーが無効になっている「ダングリングレコード」と呼ばれる、悪用され得る状態になります。

JPRS用語辞典｜dangling records（ダングリングレコード）
<https://jprs.jp/glossary/index.php?ID=0274>

ダングリングレコードはDNS検索により、外部から検出可能です。そのため、第三者がダングリングレコードを探索し、参照先の事業者にWebサーバーや権威DNSサーバーを再設定することで、サブドメインテイクオーバーやNSテイクオーバーといった、サブドメインを乗っ取るサイバー攻撃に利用される可能性があります。

▽攻撃の仕組み

サブドメインテイクオーバー・NSテイクオーバーの攻撃の仕組みについては、JPRS用語辞典の以下の項目をご参照ください。

JPRS用語辞典｜Subdomain Takeover（サブドメインテイクオーバー）
<https://jprs.jp/glossary/index.php?ID=0267>

JPRS用語辞典｜NS Takeover（エヌエステイクオーバー）
<https://jprs.jp/glossary/index.php?ID=0272>

▽攻撃の影響

第三者がサブドメインテイクオーバー・NSテイクオーバーに成功した場合、そのドメイン名を使った意図しないWebサイトの公開・フィッシング・個人情報の窃取・マルウェアの注入・クッキーの改変・なりすましメールの送信など、さまざまなサイバー攻撃に利用される可能性があります。

▼対策

▽ドメイン名の管理者における対策

サブドメインの乗っ取りを防ぐため、Webサイトを公開する際に自身の権威DNSサーバーに追加した、事業者のサーバーを参照するDNS設定は、Webサイトの公開を終了する際に、削除・変更する必要があります。

一部の事業者・研究者・専門家などから、ドメイン名の乗っ取りの被害を減らすための運用手法をまとめた文書や、攻撃可能なDNS設定が残っていないことを確認するツールなどが公開されています。こうした運用手法やツールを活用し、自身のドメイン名のDNS設定の削除・変更漏れや攻撃可能なDNS設定を検知・修正することも、有効な対策となります。

▽事業者における対策

事業者において実施可能なリスク低減策として、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・変更の確認が挙げられます。

▼参考リンク

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？
<https://jprs.jp/tech/security/2025-01-21-danglingrecords.pdf>
（本件に関するパンフレット）

サブドメインテイクオーバーの概要とその防止策
<https://www.antiphishing.jp/pdf/apc_1st_studygroup_jprs.pdf>
（第1回フィッシング対策勉強会（フィッシング対策協議会）の発表資料）

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 ～
<https://www.nic.ad.jp/sc-2021/program/sc-2021-day2-0.pdf>
（Internet Week ショーケース 2021の発表資料）

▼連絡先

本文書に関するお問い合わせは <dnstech-info@jprs.co.jp> までご連絡ください。

▼更新履歴
2025/01/21 11:00 初版作成
