# サブドメインテイクオーバー攻撃の脆弱性検知ツール SDHJChecker の開発

```
C:\Users\rakuk>sdhjchecker harugpg.shinchokudonan.com
指定されたサブドメイン :harugpg.shinchokudonan.com
処理を開始します。
発見されたCNAME:harutkue.github.io.
harutkue.github.io.:OK
OKだった場合の処理
harutkue.github.io.は適切に設定されています。
```

茨城県立IT未来高等学校
大庭悠希

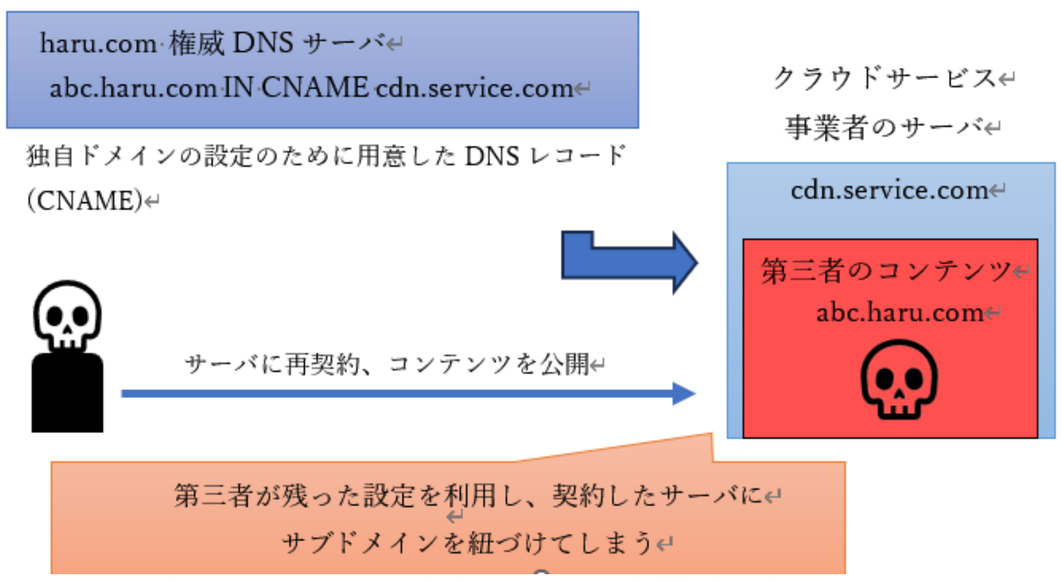
## 開発経緯

・2025年1月14日に確認された政府機関ドメイン「go.jp」が不正に扱われてしまう管理不備の事案を知った。[1]
→ドメインが乗っ取られる管理不備とはどのようなものだろうかという疑問から調べ始めた
・調べるとサブドメインテイクオーバーという攻撃の脆弱性だった→既存の対策が有用でないと知り開発し始めた。

## サブドメインテイクオーバーとは

クラウドサービスを独自ドメインで利用する際に設定したDNSレコードがクラウドサービス解約後も削除されず放置され続けていることを狙いサブドメインを乗っ取る攻撃。
→DNSレコードを解約後すぐに削除すれば対策できる。


設定したDNSレコードはクラウドサービス解約後も自動で削除されない




放置されたDNSレコードを用いて攻撃者がクラウドサービスに再契約
→不正にサブドメインを扱えてフィッシングページなどを公開できてしまう。 (JRPSの資料を参考に作成[2])

## 現状

・クラウドサービスを利用する企業が業種を問わず増加している→経験不足による不注意が増加するため自然とこの攻撃の脆弱性が増加すると考えられる。

・既存のツールでは対処が難しい攻撃である(一般的なセキュリティソフトでは対策不可・専用のツールが必要)

## 脆弱性検知

・検知するべき脆弱性はクラウドサービス用の設定があるDNSレコードが存在している かつ クラウドサービスを解約している状態となる

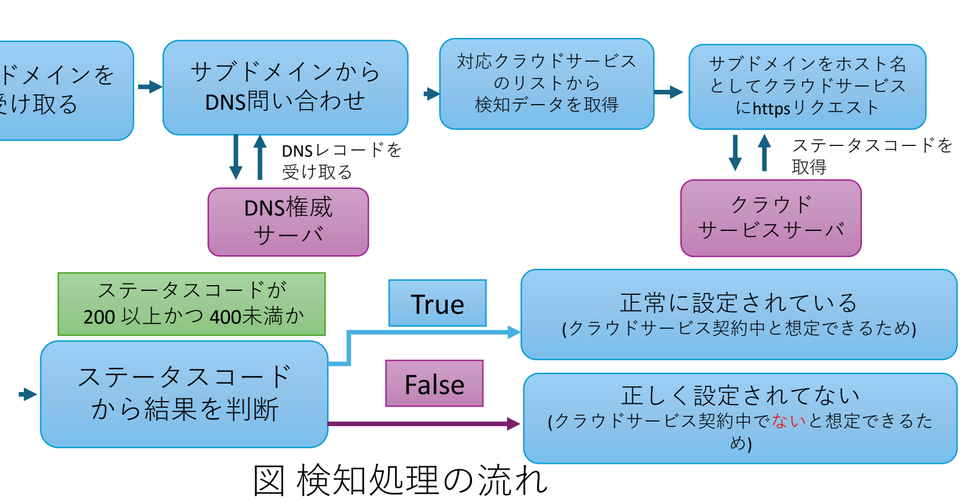



図 検知処理の流れ

### 実際の検知例

```
sdhjchecker harugpg.shinchokudonan.com
```

**適切に設定されている状態**

```
C:\Users\rakuk>sdhjchecker harugpg.shinchokudonan.com
指定されたサブドメイン :harugpg.shinchokudonan.com
処理を開始します。
発見されたCNAME:harutkue.github.io.
harutkue.github.io.:OK
OKだった場合の処理
harutkue.github.io.は適切に設定されています。
続行するには何かキーを押してください . . .
```

**適切に設定されていない状態**

```
C:\Users\rakuk>sdhjchecker harugpg.shinchokudonan.com
指定されたサブドメイン :harugpg.shinchokudonan.com
処理を開始します。
発見されたCNAME:harutkue.github.io.
harutkue.github.io.:NG
NGだった場合の処理
harutkue.github.io.は適切に設定されていません！
続行するには何かキーを押してください . . .
```

## 工夫点

・コマンド引数にサブドメインを指定するだけで実行できる簡素さ
・将来のライブラリ化を見据えコア部分とCLI部分を分離したこと

## 今後の予定

・クラウドサービス対応数を増やすためにユーザからのリクエストで検知可能なクラウドサービスを増やす自動化を実装する
・複数ドメインの入力対応・一つのドメインから複数のサブドメインを取得する機能などを実装する

## 活用方法

・定期的に実行することで状態を定期的に監視する
・気になったらすぐ入力して実行できる
→DNS管理に慣れていない企業や人に!

## 参考文献

[1] 日経 Xtech 2025年2月26日
政府機関の「go.jp」を使うWebサイトを第三者が設置、設定ミスを突く悪用手口
https://xtech.nikkei.com/atcl/nxt/column/18/00001/10169
[2] JRPS サブドメインテイクオーバー
https://jprs.jp/glossary/index.php?ID=0267