D1-4 サブドメインテイクオーバーの仕組みと実践的な対策について

Internet Week 2025 2025/11/26
NTTドコモビジネス株式会社
髙田 美紀・竹﨑 彬隼

$ whoami

NA4Sec Network Analytics for Security

つなごう。驚きを。幸せを。 docomo Business

名前

- 髙田 美紀 (たかた みき)

本業

- NTTドコモビジネス株式会社
  デジタル改革推進部 データドリブンマネジメント推進部門
- 2020年より現職、社内向けデータ分析基盤の設計・開発・運用に従事

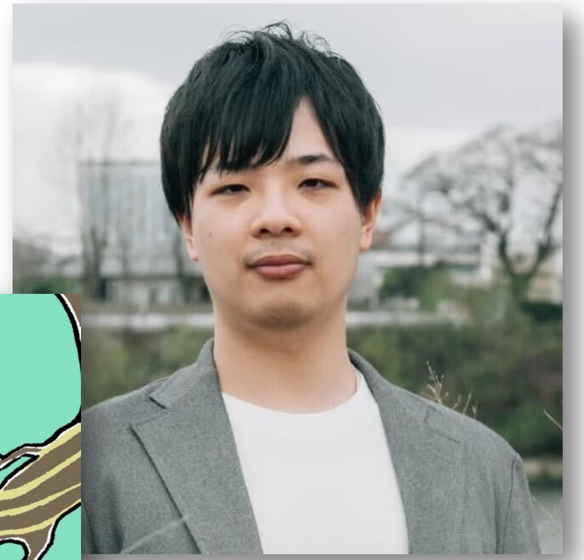
対外活動

- 2005年ごろ JEAG (Japan Email Anti-Abuse Group) 幹事
- 2009年より DNSSECジャパン 広報WG リーダー
- 2012年より日本DNSオペレーターズグループ 幹事
- JPNIC主催 InternetWeek プログラム委員
- 2024年 JPAAWG 7th General Meeting 講演「ドメイン名の終活について」
- 2025年 第29回 サイバー犯罪に関する白浜シンポジウム BoF 座長

$ whoami

名前

- 竹﨑 彬隼（たけざき あきとし）



本業

- NTTドコモビジネス株式会社 イノベーションセンター
  Network Analytics for Security (NA4Sec) PJ
- セキュリティ技術研究・開発（攻撃インフラの脅威分析）

対外活動

- AVTOKYO2024「Going down the RAT hole: Deep dive into the Vuln-derland of APT-class RAT Tools」
- CODE BLUE2025 CyberTAMAGO

アジェンダ

- 背景
- サブドメインテイクオーバーの原理（CNAMEテイクオーバー）
- サブドメインテイクオーバー対策
- 会社・組織内での対策
- サブドメインテイクオーバーの実践的な対策
- 組織のサブドメインを把握するのはなぜ難しいのか
- 「現実的な」サブドメインテイクオーバーに気付く仕掛けの例
- まとめ
- 参考資料

NA4Sec
Network Analytics for Security

つなごう。驚きを。幸せを。
docomo Business

背景

ドメイン名を安易に手放すことによるリスクは

広く認知されるように

プレミアムフライデーの偽サイトに経産省が注意喚起 手放したドメイン、第三者が利用か

2025年11月20日 13時26分 公開

[芹澤隆徳，ITmedia]

印刷 見る Share B! 34 0

経済産業省は11月19日、かつての「プレミアムフライデー推進協議会」のドメインを取得した第三者が類似したホームページを開設しているとして注意喚起した。いわゆるドロップキャッチの事例とみられる。

かつての「プレミアムフライデー推進協議会」WebサイトのURLを入力すると出てくる類似ページ

経済産業省は、当該サイトはプレミアムフライデー推進協議会や制度とは一切関係ないとしている。このサイトにアクセスすると「場合によっては、コンピュータウイルスに感染したり、入力情報が不正に取得されたりする等のおそれ」があるとしてアクセスしないように呼び掛けた。また当該URLのリンクを掲載しているWebサイトに対して、削除するように求めている。

https://www.itmedia.co.jp/news/articles/2511/20/news093.html

しかし実は

ドメイン名を手放していなくても

悪用されるリスクが

- 2024年末から2025年初にかけて「省庁のドメインが不正利用された」といった報道が相次ぐ
- デジ庁がドメイン管理ガイドラインを改定する事態にまで発展

このときに使われた手法が
サブドメインテイクオーバー

「go.jp」サイトを第三者が設置

狙われるサブドメイン　変換設定の削除し忘れに注意

玄 忠雄　日経コンピュータ

2025.02.26

全2642文字

デジタル庁は2025年1月14日、政府機関のドメインである「go.jp」に管理の不備が確認されたとして、全省庁に対して状況の確認と対策を要請したことを明らかにした。ドメインが不正利用できる状態にあったのは国土交通省や総務省、厚生労働省などだ。

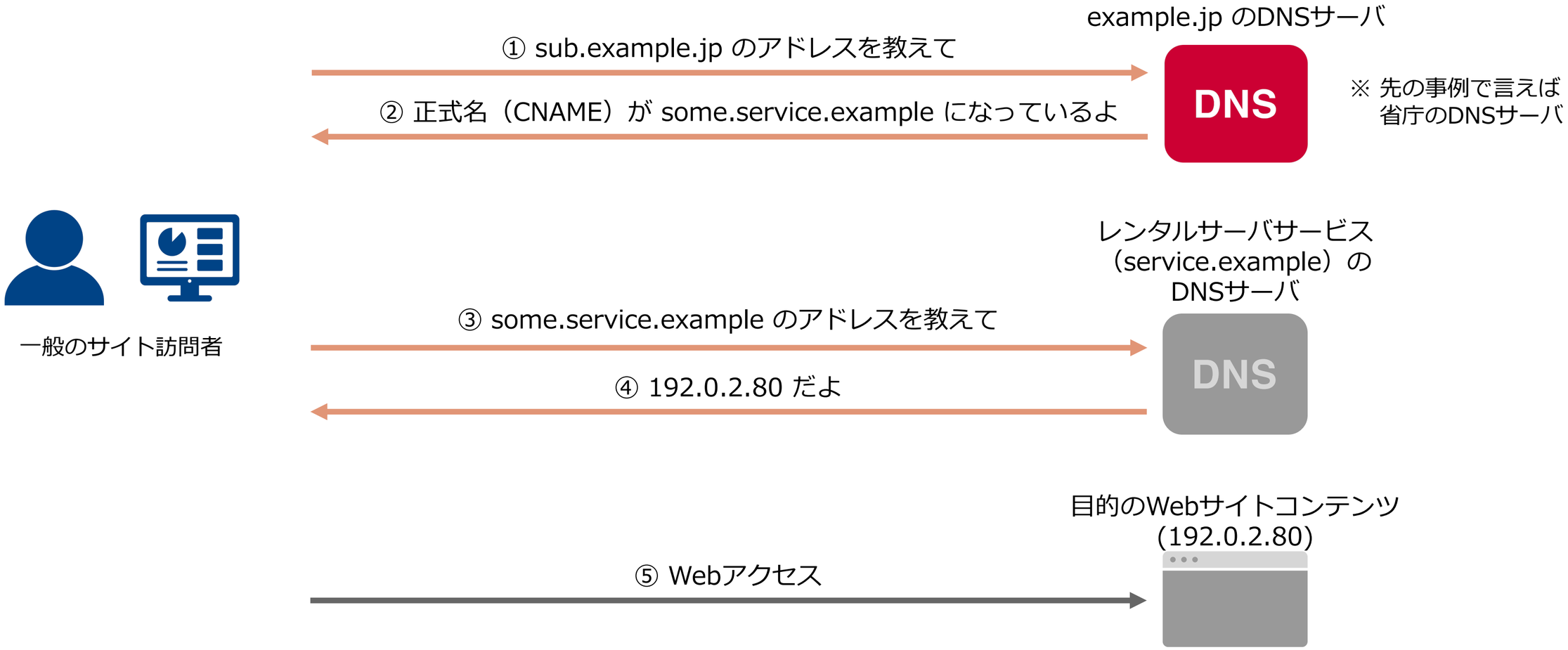
このうち国交省が大都市交通センサスの調査サイトで使ったドメイン「daitoshi.mlit.go.jp」では、第三者がこれを使って海外のオンラインカジノに誘導する広告サイトを開設していた。総務省では、新型コロナウイルス対策における特別定額給付金の広報活動に使ったドメイン「kyufukin.soumu.go.jp」が不正利用できる状態にあった。

https://xtech.nikkei.com/atcl/nxt/mag/nnw/18/041800012/021700277/

サブドメインテイクオーバーの原理（CNAMEテイクオーバー）

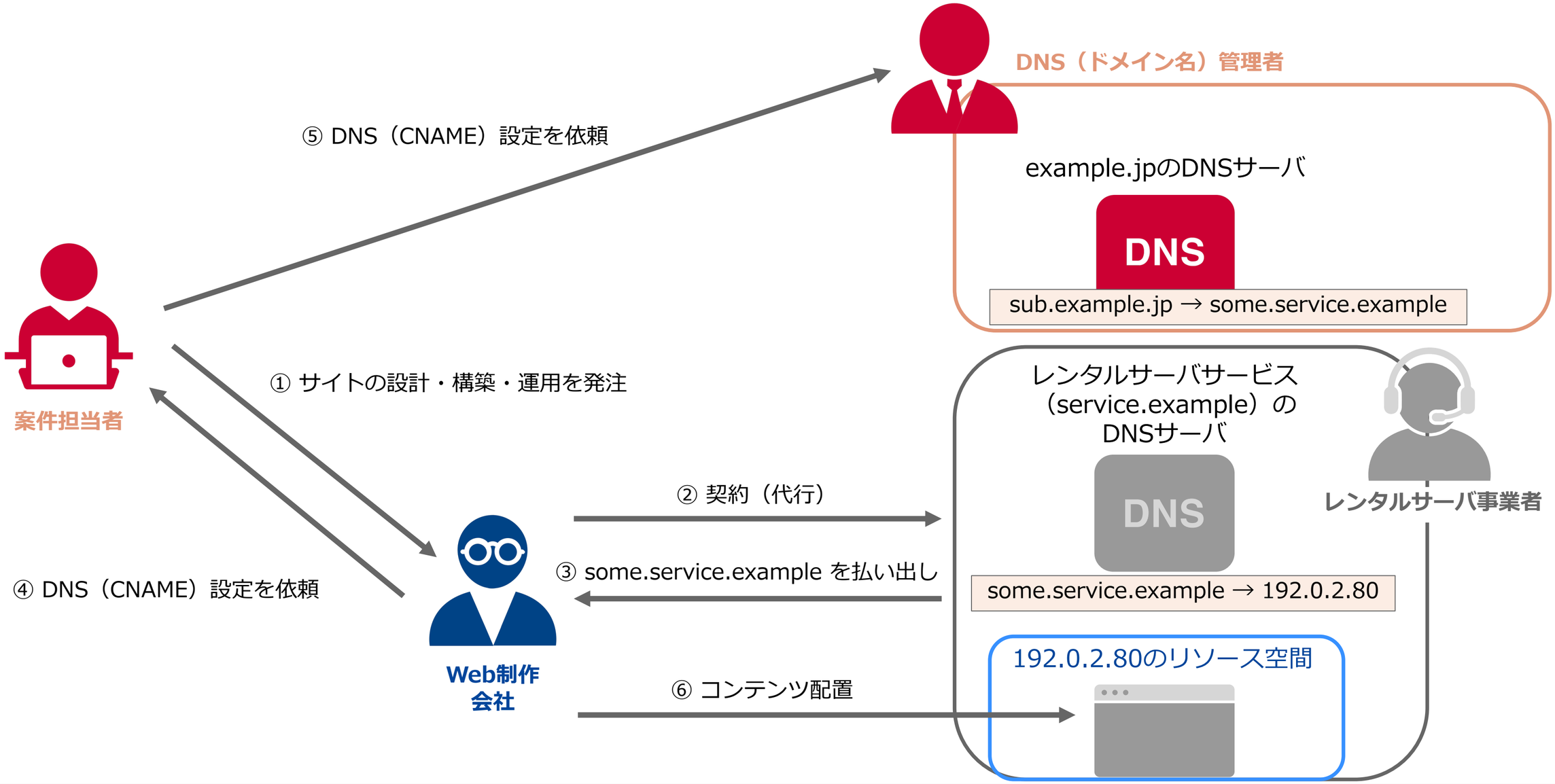
前提：正規サイト運用時のアクセス挙動

例：
外部のレンタルサーバサービス（service.example）を使って
Webサイト（sub.example.jp）が構築されているケース



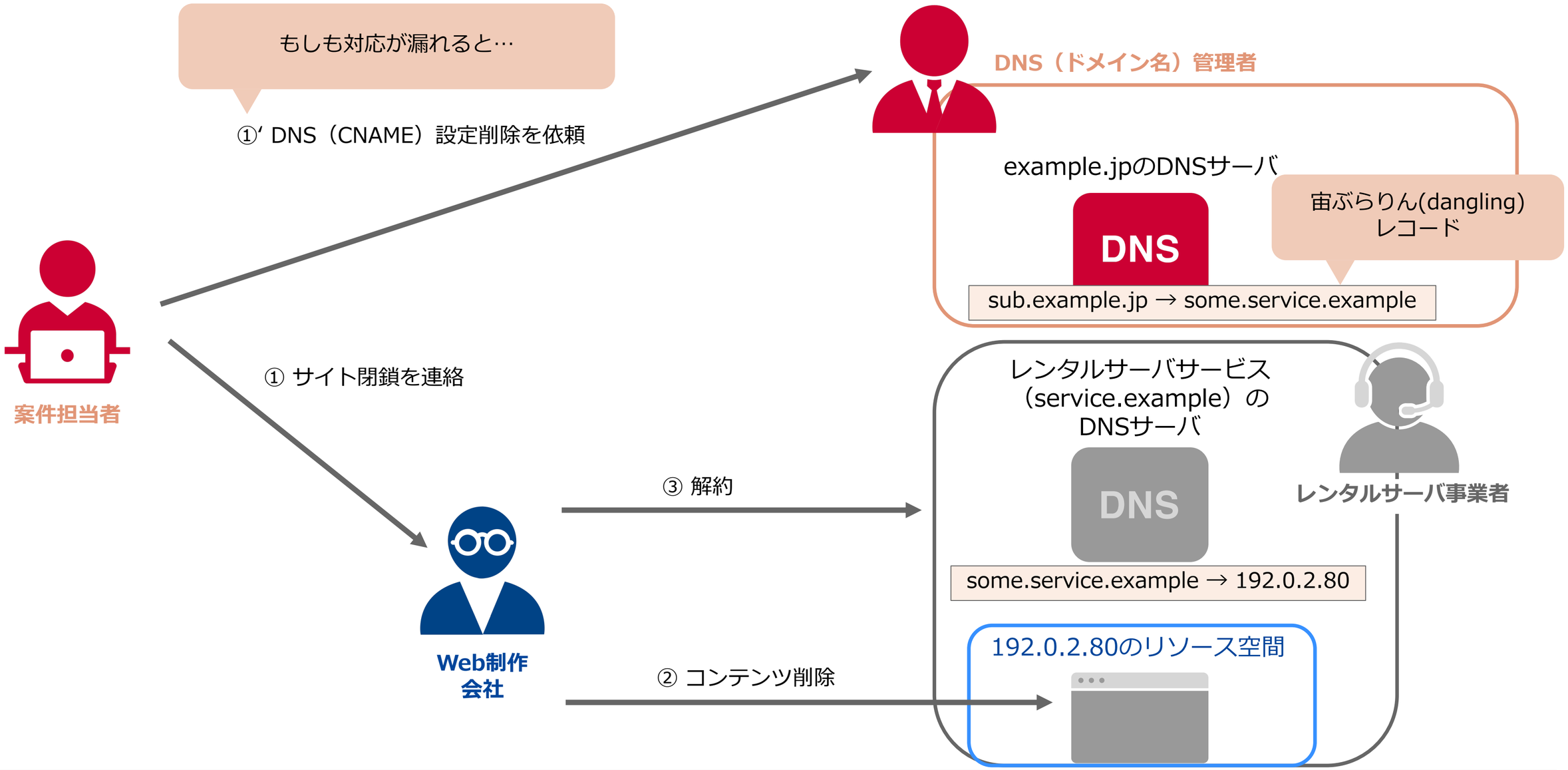
注：説明を簡単にするため、厳密な用語を使っていなかったり、RFCに沿っていなかったりする部分があります

Webサイト構築のありがちな流れ（外注）



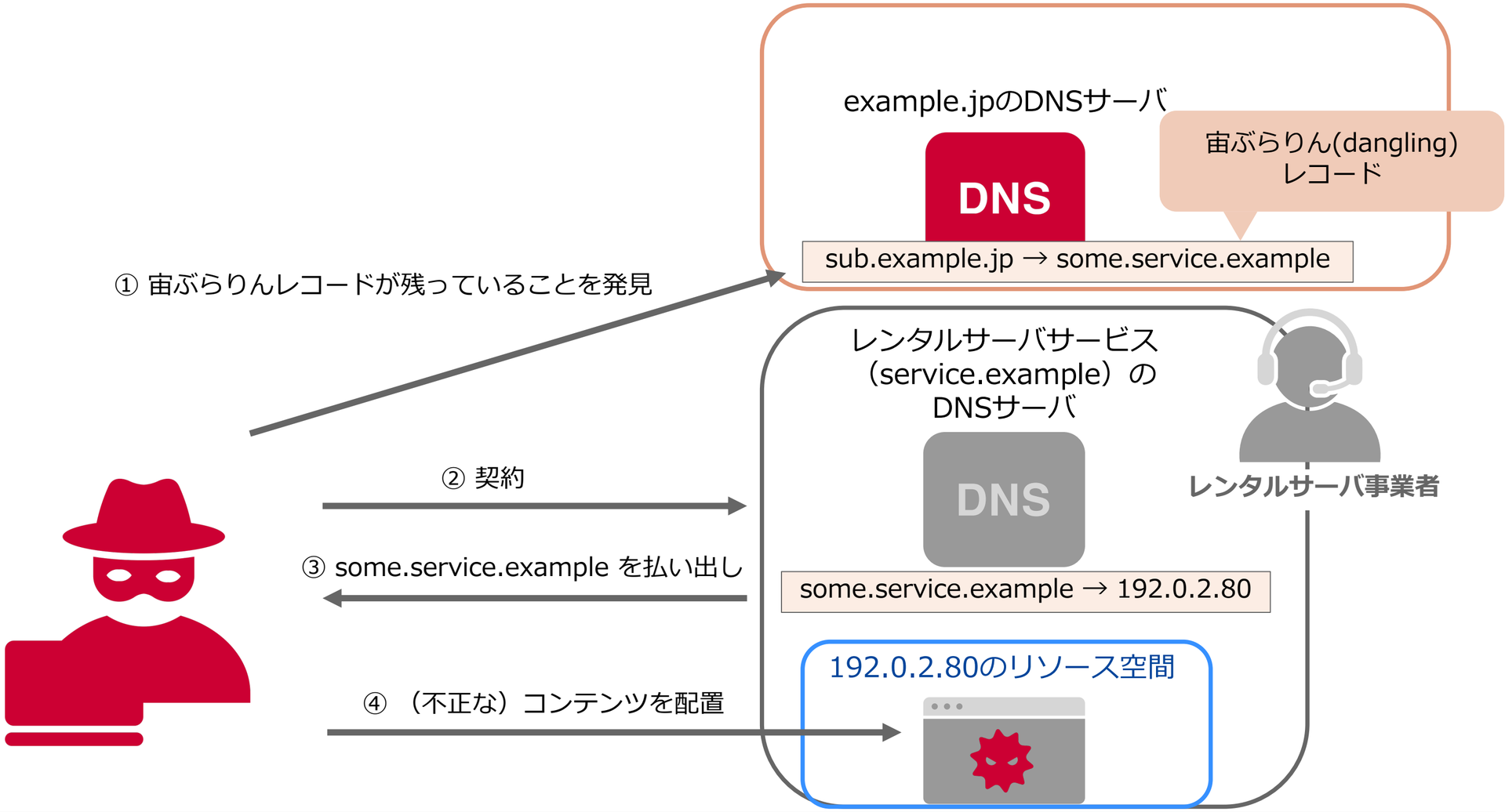
注：要点に絞って簡略化しています

Webサイト閉鎖時の流れ



注：要点に絞って簡略化しています

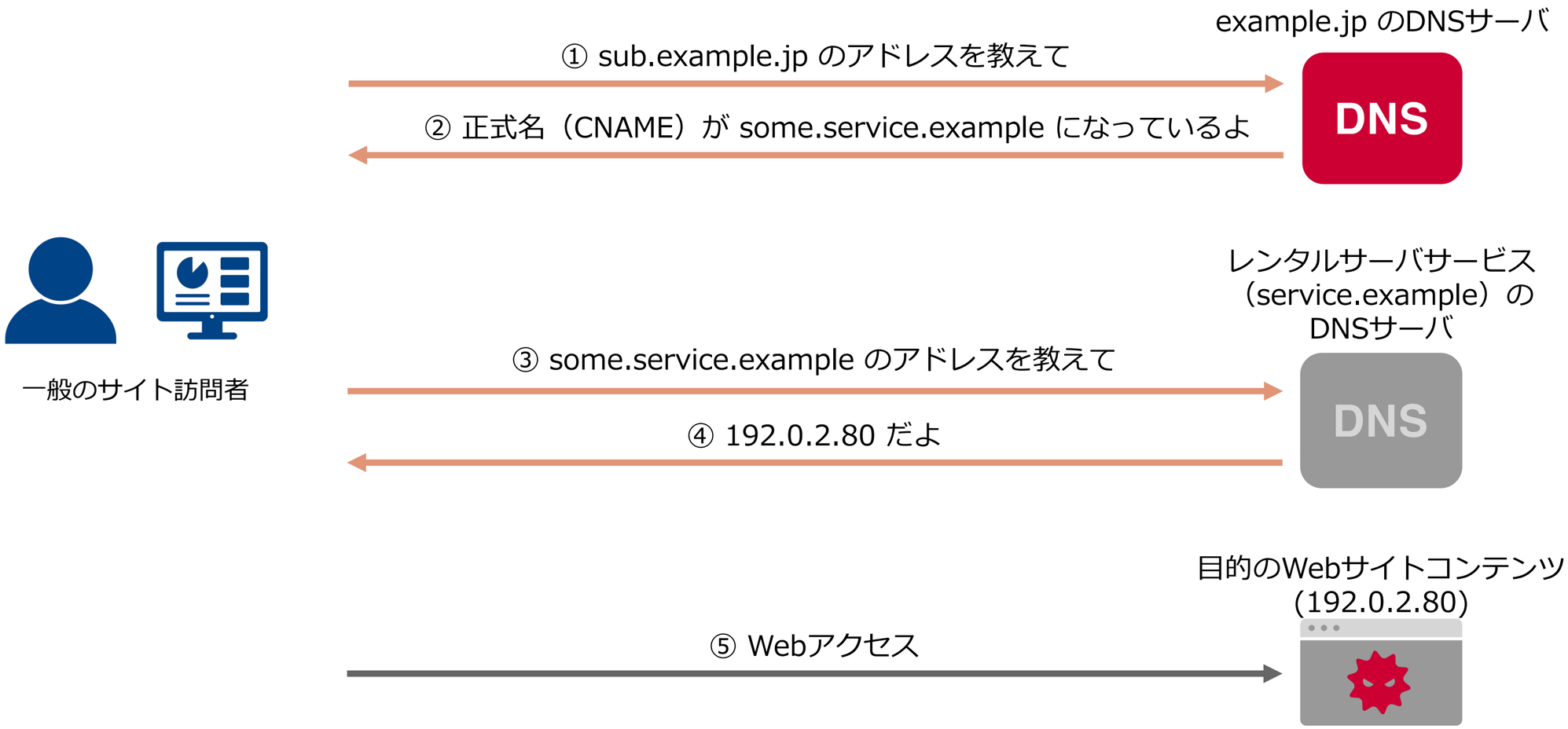
サブドメインテイクオーバー



注：要点に絞って簡略化しています

テイクオーバー後

サイト訪問者には **sub.example.jp のWebサイトが不正な内容に書きかわっている** ように見える



注：説明を簡単にするため、厳密な用語を使っていなかったり、RFCに沿っていなかったりする部分があります

攻撃者側の動機

NA4Sec Network Analytics for Security

つなごう。驚きを。幸せを。 NTT docomo Business

動機：なぜこんな攻撃をするのか?

- 手っ取り早く、PVを稼ぎたい!!
    - 不正なコンテンツではSEO対策がしづらい
- 官公庁のキャンペーンサイトは多くの場所からリンクされており、多くの流入が見込まれる

- または、もっと悪意のある攻撃の場合もあるかもしれない
    - フィッシングなど
    - アクセスしてきた人の情報を搾取するもの
    - 企業のブランド侵害

サブドメインテイクオーバー対策

基本的な防止策（考え方）

サブドメインテイクオーバーリスクの本質は「**片付け忘れ**」

- **サービスやサイト終了時には「原状回復」**
  - コンテンツの追加 → コンテンツの削除
  - DNS設定の追加 → DNS設定の削除

- DNSレコードが**宙ぶらりんの状態（Dangling Records）**になっていると危険

NA4Sec
Network Analytics for Security

つなごう。驚きを。幸せを。
docomo Business

とは言え、
（特に）どこに気をつければよいのか

大前提
「外部サービスとの連携」

気をつけた方がよいサービス
~ Dangling CNAMEのテイクオーバーリスク ~

NA4Sec Network Analytics for Security

つなごう。驚きを。幸せを。
docomo Business

△△△.service.example

任意の名前やユーザ名など　　外部サービスのドメイン名

自分たちのドメイン名（***.example.jp）を
このような形式のFQDNに紐づける構成が出てきたら要注意
（特にサービス利用者が「△△△」部分をコントロールできるサービス）

設定するDNSレコードのイメージ

```
***.example.jp.  IN  CNAME  △△△.service.example.
```

代表例

サービス名	テイクオーバーされるかもしれないドメイン名	
AWS S3	*.s3.amazonaws.com	
Microsoft Azure	*.cloudapp.net *.cloudapp.azure.com *.azurewebsites.net *.blob.core.windows.net *.cloudapp.azure.com *.azure-api.net *.azurehdinsight.net *.azureedge.net *.azurecontainer.io	*.database.windows.net *.azuredatalakestore.net *.search.windows.net *.azurecr.io *.redis.cache.windows.net *.azurehdinsight.net *.servicebus.windows.net *.visualstudio.com
さくらのレンタルサーバ	*.sakura.ne.jp	
Bitbucket	*.bitbucket.io	
AWS Elastic Beanstalk	*.elasticbeanstalk.com	
Ngrok	*.ngrok.io	
Readme.io	*.readme.io	
Readthedocs	*.readthedocs.io	
はてなブログ	*.hatenablog.com	

ここに挙げたのは一例です

NA4Sec
Network Analytics for Security

つなごう。驚きを。幸せを。
docomo Business

ただし…

Dangling CNAME対策の落とし穴

△△△.service.example

任意の名前やユーザ名など　　外部サービスのドメイン名

「△△△」部分を第三者に取られなければ大丈夫
．．．とは限らない

サービス仕様によっては「△△△」部分を自分たちが押さえている状態でも
テイクオーバーが成立する場合がある

例：GitHub Pages (*.github.io)

GitHub Pages

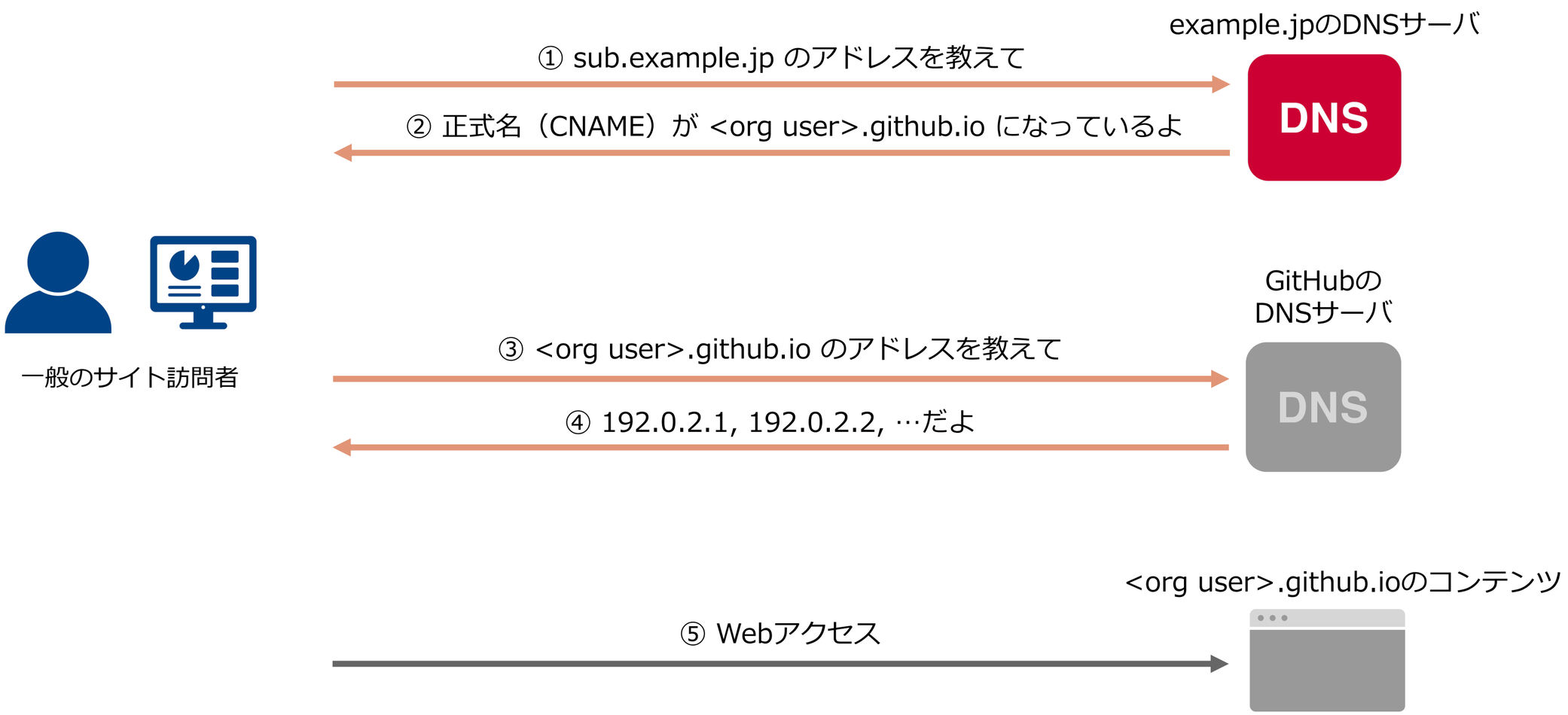
- GitHubが提供する静的サイトホスティングサービス
  - GitHubリポジトリから静的なWebサイトを直接ホストできる
- *****.github.io の「*****」部分はGitHubユーザー（あるいはOrganization）アカウント名
  - **アカウントを手放さない限り**は第三者がその名前を使うことはできない
- github.ioドメイン（*****.github.io）をそのまま使う方法の他に**カスタムドメイン**でもホストできる
  - 別名（**CNAME**）を使う構成 (sub.example.jp → *****.github.io)

特定の条件が揃うと**アカウントを手放していなくても第三者によるテイクオーバーが可能**

1. *****.github.io に向けたCNAMEレコードが残っている
   （Dangling CNAME）

2. カスタムドメインの検証未実施（デフォルト）

GitHub Pagesへのアクセス



注：説明を簡単にするため、厳密な用語を使っていなかったり、RFCに沿っていなかったりする部分があります

GitHub Pagesへのアクセス

一般のサイト訪問者

example.jpのDNSサーバ

① sub.example.jp のアドレスを教えて

② 正式名（CNAME）が <org user>.github.io になっているよ

DNS

GitHubの
DNSサーバ

③ <org user>.github.io のアドレスを教えて

④ 192.0.2.1, 192.0.2.2, …だよ

DNS

⑤ Webアクセス

404 Not Found

ページの公開をやめたら、
エラーページが表示される

注：説明を簡単にするため、厳密な用語を使っていなかったり、RFCに沿っていなかったりする部分があります

GitHub Pagesテイクオーバー

- （不正な）コンテンツを <mal user>.github.io に配置
- <mal user>.github.io のカスタムドメインとして **sub.example.jp** を設定

[ポイント1]
未検証のドメインについては、**誰でもカスタムドメインとして任意のFQDNを指定可能**

example.jpのDNSサーバ

DNS

DNS（CNAME）レコードが残ったまま

sub.example.jp → <org user>.github.io

GitHubの
DNSサーバ

DNS

GitHub Pagesサーバ

<org user>.github.ioのコンテンツ

<mal user>.github.ioのコンテンツ

注：説明を簡単にするため、厳密な用語を使っていなかったり、RFCに沿っていなかったりする部分があります

GitHub Pagesテイクオーバー

一般のサイト訪問者

example.jpのDNSサーバ

① sub.example.jp のアドレスを教えて

② 正式名（CNAME）が <org user>.github.io になっているよ

DNS

sub.example.jp → <org user>.github.io

GitHubの
DNSサーバ

③ <org user>.github.io のアドレスを教えて

④ 192.0.2.1, 192.0.2.2, …だよ

DNS

[ポイント2]
GitHub PagesのDNSサーバは**あらゆる *.github.io について同じアドレスを返す**

GitHub Pagesサーバ

<org user>.github.ioのコンテンツ

⑤ Webアクセス

[ポイント3]
GitHub Pagesは**正しいCNAMEを経たアクセスかどうかは検証しない**（できない）

<mal user>.github.ioのコンテンツ

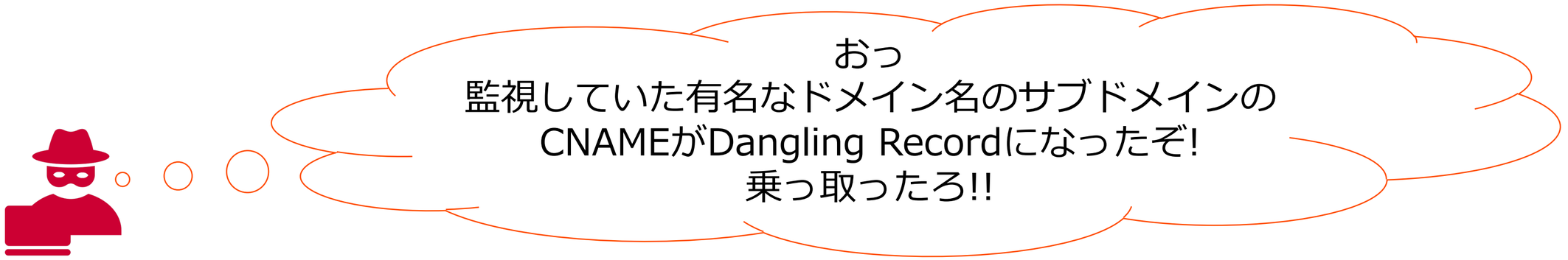
[ポイント1]
未検証のドメインについては、**誰でもカスタムドメインとして任意のFQDNを指定可能**

注：説明を簡単にするため、厳密な用語を使っていなかったり、RFCに沿っていなかったりする部分があります

アクター視点

- ユーザーがGitHub Pagesを公開すると、GitHubがCAを通じ、HTTPSの証明書を発行
- CAは証明書をCertificate logsに登録
- アクター
    - Certificate logsのcommonNameを見て、DNS検索し、GitHub PagesへのCNAMEとなっているのを発見
    - ページをwatchし続け、下記のような状況を待つ
        - HTTP Status Code: 404
        - CNAME/Aが残っている (Dangling)
    - カスタムドメインの設定をしてみて、ドメインが保護されていなければ、テイクオーバーの準備完了

攻撃者はこの状態になることを**ずっとクロールして監視👀している**



GitHub Pagesテイクオーバー対策

対策は**GitHubだけでは完結させられない**のが現状

- 現状、GitHub PagesではEnterpriseユースとしてカスタム (独自) ドメインの利用は想定されていない

- 管理者としてはガードレールがほしい。でも
  - 自組織のOrganizationにドメイン検証を強制することはできない
    - ドメイン検証すれば、CNAMEレコードの消し忘れがあったとしても、第三者が使うことはできないのだが…
  - Enterpriseレベルでカスタムドメイン設定を禁止することもできない
    - 危険なので、独自ドメインの設定をできないようにしたいが、それもできない

- そもそも、**ドメイン検証しなくても任意の FQDN を設定できる**って仕様ってどうなの?
- GitHubはこの件を認知しているが、優先度は低いとのこと
  - 「(特に課金)ユーザーからのリクエストが多くなれば優先度が上がる」そうなので、みなさんケース作成してください!

GitHub Pagesテイクオーバー検知

検知方法1

- 自社ドメイン名のCertificate logsを監視
- commonNameを見て、DNS検索し、GitHub PagesへのCNAMEとなっているのを発見
- ページをwatchし続け、下記のような状況になっていないか監視
    - HTTP Status Code: 404
    - CNAME/Aが残っている
- そうなってしまっていたらインシデント対応開始

検知方法2

- 改ざん検知ツール、Google Search Consoleでの警告などを利用

大事なこと

- インシデント発生時の連絡体制を取っておくこと
- そのサブドメイン名はどの組織が管理しているか?
    - Danglingを検知してからは、**攻撃者との競争**です。

GitHub Pagesテイクオーバー検知

NA4Sec Network Analytics for Security

つなごう。驚きを。幸せを。 docomo Business

検知方法1

- 自社ドメイン名のCertificate logsを監視
- commonNameを見て、DNS検索し、GitHub PagesへのCNAMEとなっているのを発見
- ページをwatchし続け、下記のような状況になっていないか監視
    - HTTP Status Code: 404
    - CNAME/Aが残っている
- そうなってしまっていたらインシデント対応開始

検知方法2

- 改ざん検知ツール、Google Search Consoleでの警告などを利用

大事なこと

- インシデント発生時の連絡体制を取っておくこと
- そのサブドメイン名はどの組織が管理しているか?
    - Danglingを検知してからは、**攻撃者との競争**です。

これは事後対策でしかない

会社・組織内での対策

社内での啓発活動

- 各社・各組織ではSaaSの利用が進んでいるのではないでしょうか
    - GitHub Pagesに限らず、「気をつけた方がよいサービス」で紹介したようなもの

- 抜け漏れなく管理するためには、全てのSaaS利用を統括組織で一括管理する案もありますが、現実的ではないでしょう
- スピード感を持って業務を進めるためには、利用者側のリテラシー向上が必須です
    - 社内での啓発活動、e-learningなど

要点を絞って伝える

- ドメイン名は会社の看板である
- 会社の看板たるドメイン名で違法サイトを開設されるのは、非常に高リスク
    - フィッシングサイト
    - 違法コンテンツへの誘導サイト
    - など
- 第三者に不正利用されたら、報道発表が必要になる事態に発展する可能性もある
- そのためには「DNSレコードの管理」「後片付け」が重要

サブドメインテイクオーバーの実践的な対策

おさらい

NA4Sec Network Analytics for Security

つなごう。驚きを。幸せを。 docomo Business

サブドメインテイクオーバーリスクの本質は「**片付け忘れ**」

- **サービスやサイト終了時には「原状回復」**
  - コンテンツの追加 → コンテンツの削除
  - DNS設定の追加 → DNS設定の削除

- サブドメインテイクオーバーを起こさないためには、~~各部署に”**ちゃんとして**”もらえば良い。~~

そんなことは**不可能**

各部署にお願いしても・・・

- 「忙しくて忘れてました！」
- 「CNAME？ 何ですかそれは？」
- 「そういうのは委託会社に任せているので…」
- 「うちはそういう設定してないと思います。」

能動的に**見つけに行く**しかない

とは言え、見つけに行くって、何をすればいの？

対策のために必要な要素

サブドメインの把握

- 今、**実際に使われている**サブドメインを把握する

定期監視

- 人が頑張るのではなく、機械的、定期的に監視する

発見後の対処

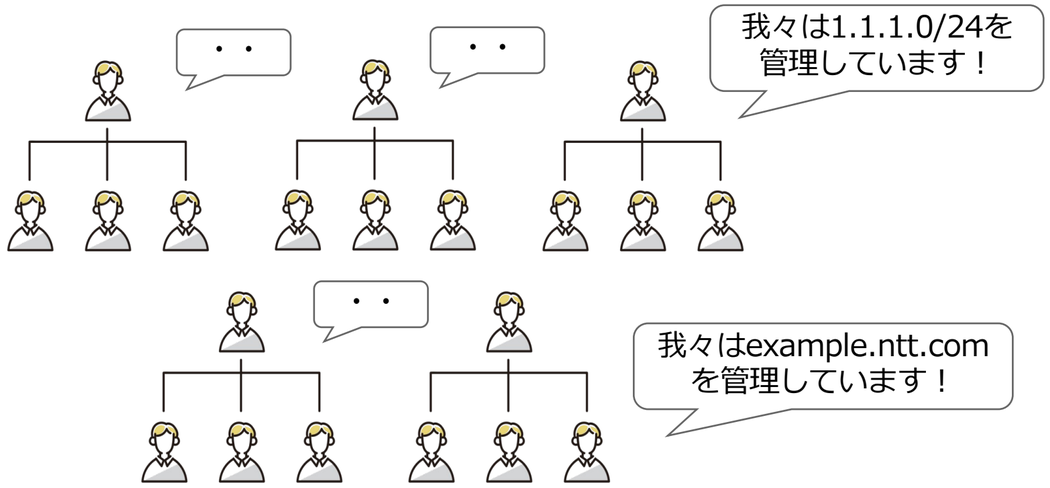
- 人が気をつけるのではなく、機械的に監視する

これ、なんか難しそうじゃない？

組織のサブドメインを把握するのはなぜ難しいのか

サブドメイン管理の現実

サブドメインのリスト化は Excel や とあるDNS のレコードを見るだけでは**終わらない**



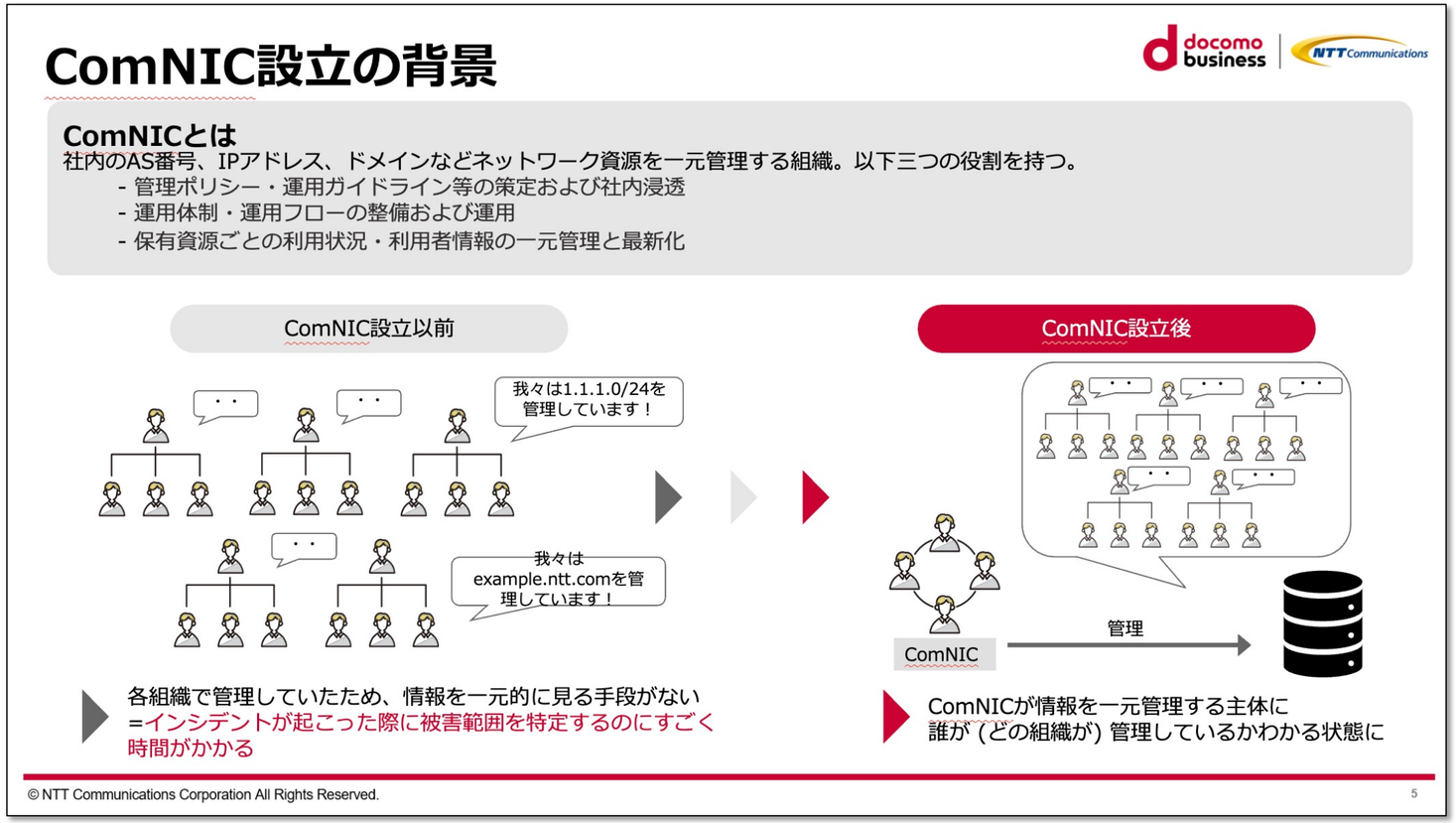
- 複数の部署・子会社・委託先が、それぞれ**勝手にサブドメインを発行**している
- 各クラウド（AWS / GCP / Azure 等）で**別々**にDNS設定が行われている
- n年前のプロジェクトで作ったサブドメインが、担当者退職後も**そのまま残っている**
- 台帳にない**野良サブドメイン**が見つかる or　台帳には記載されているのに**サービス終了済み**

サブドメイン把握を難しくする本質的な要因

結局のところ、**管理者が分散している**ことが原因

対策編:弊社の場合

ComNICと呼ばれる組織を設立した。



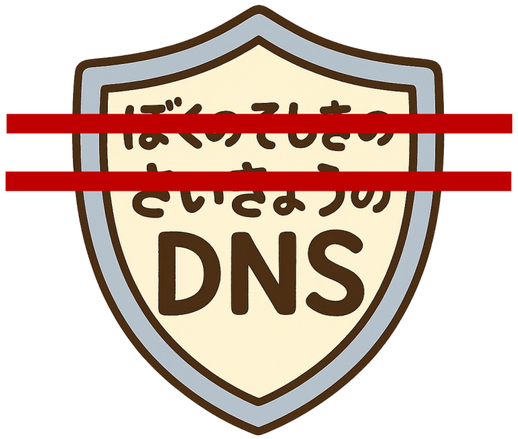
引用:InternetWeek2024_D2-6 「使後の世界 ～利用終了した独自ドメインのその後～」

対策編:弊社の場合

ComNICによって、
対象のドメインさえわかっていれば「**誰に聞けばいいか**」はわかる状態に。

なぜレコードの完全把握をやらないのか？

会社が使用する全てのDNSレコードを「ぼくのそしきのさいきょうのDNS」に委譲すれば把握できるが、
およそ現実的ではない。



現実的には

- 「**見える範囲**」**からアプローチ**するしかない。
- 逆に言うと、見えた範囲には確実にアプローチできるようにしておく。

「現実的な」
サブドメインテイクオーバーに気付く仕掛けの例

対象にするサブドメインの収集

- 対象にするサブドメインは「**見える範囲**」からアプローチするしかない。

弊社の場合

インシデント対応等のために EDRログ、Webプロキシログなどを取得して分析できる環境が存在

社員が日常でアクセスしているサブドメインから、アプローチを始めた。

これらを対象に、**定期監視**を始めていく。

監視手法そのいち:
HTTPステータスコードベースの監視

NA4Sec Network Analytics for Security

つなごう。驚きを。幸せを。
docomo Business

手法

- 監視対象のサブドメインのHTTPステータスコードを定期的に取得
- 「**404**」になった / なっているものがあれば状況を確認

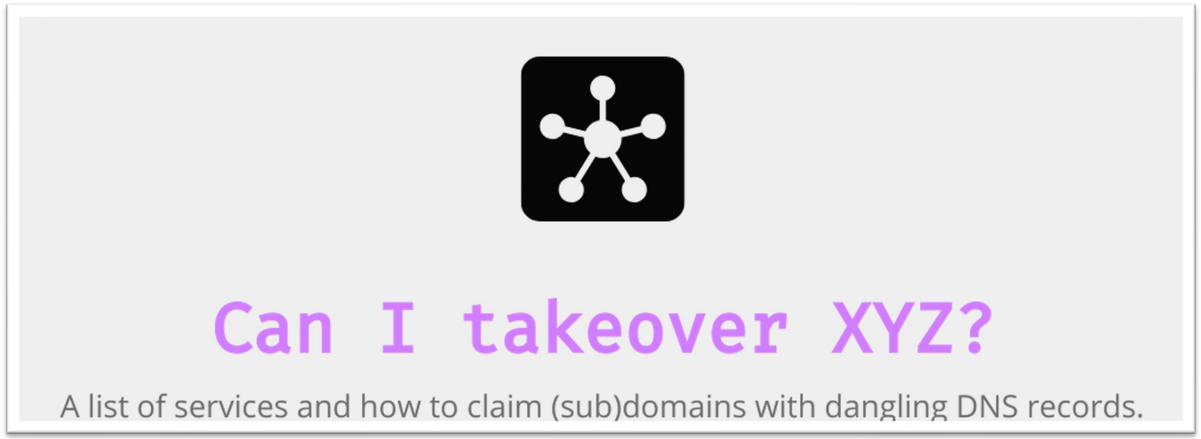
確認すること

- 対象はWebページかどうか
- 意図した404かどうか
    - 例えば、開発環境でアクセス制限をかけている場合、外部から404として見えても正常だったりする
- CNAME先のサービス、および設定は**テイクオーバーに関して脆弱かどうか**
    - そもそも対策されているサービスも多い

なぜ404を確認するのか

- サブドメインが404になっている状態とは？
  - 正規コンテンツの利用が終了している状態
  - 外部連携しているサービスが「片付け」されていなければ**テイクオーバーの危機**！？（=**dangling**）

攻撃者も同じところを着目している



https://github.com/EdOverflow/can-i-take-over-xyz

攻撃者がテイクオーバーに対して脆弱なサイトを探すときに、
404固有のレスポンスをFingerprintにする例も多く見られる

監視手法そのに:
コンテンツ変化監視

NA4Sec Network Analytics for Security

つなごう。驚きを。幸せを。
docomo Business

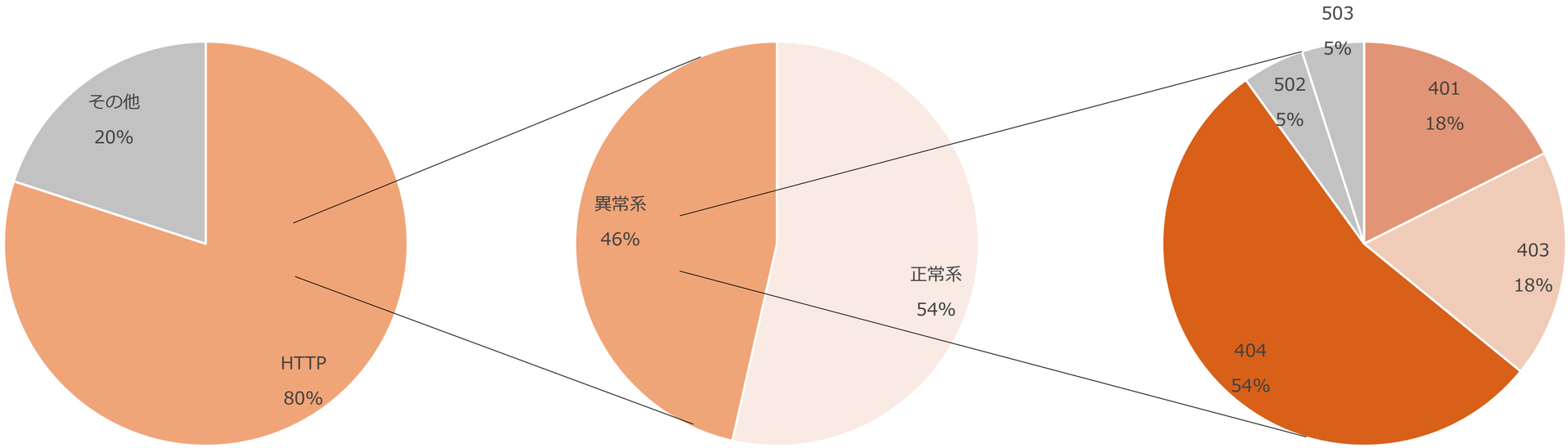
前提

- 基本は前述の「**HTTPステータスベース**」で監視したい
- ステータスが404になっていないが気付きたい一部のケースに対応する為の監視
    - 副次的に過去の状況がわかりやすくなって調査が捗る効果も

気付きたいケース

- **ホスティングサービス**等のコンテンツが表示されている状態
    - 404ではなく他のステータスコード（200、403等）でコンテンツの消失を示すようなサービスの場合
- （例えばオンラインカジノみたいな）**意図していないページ**が表示されている状態

システムを運用して見えてきたもの



- HTTPプロトコルで応答するもののうち、最終的に404を返すのは2割程度だった
  - 意外と確認するべきサブドメインの数は**減らすことができる**

システムを運用して見えてきたもの

NA4Sec Network Analytics for Security

つなごう。驚きを。幸せを。 docomo Business

やりたかったこと

- 見えているサブドメインのリストからリスクのあるサブドメインを発見する。

結果

- 前半パートで取り上げたGithub Pagesへの**dangling CNAMEを発見**した。
  - 管理者にヒアリングしたところ幸い対策済み
    - Github Pagesの例では、カスタムドメインの検証設定をすることで対策可能
  - 実際にテイクオーバー出来ないことも確認

▼

この手法の**有効性を確認**

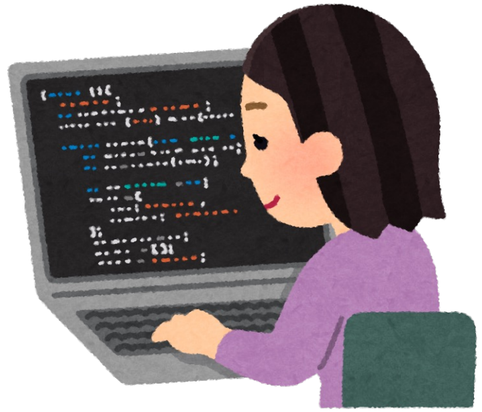
見つけた後の連携が最重要

検知だけで終わらせないための体制が重要。

弊社の場合

- DNSに知見のある人が集まるSlackで初動共有
- そこから担当部署への連携が実施される

できれば検知 → 報告 → 修正の流れを標準化したいところ



NA4Sec
Network Analytics for Security

つなごう。驚きを。幸せを。
docomo Business

まとめ

まとめ

📌 背景

- 官公庁サイト等が乗っ取られ詐欺・広告に悪用されていた

🛠️ 攻撃（サブドメインテイクオーバー）手法

- 放置されたCNAME/NSレコード (Dangling Records) を悪用
    - Certificate logsなど外部から確認できる情報をもとにクローリング
- 委任先ドメイン名を第三者が取得し不正コンテンツを配置

🛡️ 気をつけよう

- 自分たちのドメイン名を ******.service.example. のような**外部のFQDNに紐づける**構成 (CNAME)
- 自分たちのドメイン名の**サブドメイン管理を外部サービスに委任する**構成 (NS)
- **あと片付けをしっかり。**不要になったら、CNAME/NSを削除 (登録を管理しておきましょう)
- 技術的に縛ることができない場合があるため、自社ドメインを監視する・社内での啓発活動も大事

サブドメインテイクオーバーにまつわる最近の脅威事例

最近の脅威事例

- 総務省の Dangling (宙ぶらりんな) CNAME を保護した話
- (続) 総務省の Dangling (宙ぶらりんな) CNAME を保護した話（2024/12/23 & 30, 鈴木常彦先生）
  - 2024年末の中央省庁系ドメイン名がサブドメインテイクオーバーされうる状態にあった
  - サブドメインテイクオーバーされるリスクのあったサービス：**さくらのレンタルサーバ**
  - NSテイクオーバーされるリスクのあったサービス：
    heteml、**XServer**、**XServerビジネス**、**さくらインターネット（ネームサーバサービス）**、**AWS Route 53**

- 8 Million Requests Later, We Made The SolarWinds Supply Chain Attack Look Amateur (2025/2/4, WatchTowr)
  - 利用後廃止された150個の**AWS S3**バケットを再設定し、経過観察したところ2ヶ月で800万リクエストが集まった
    - 世界各国の政府系ネットワーク、アメリカ軍事系ネットワーク、Fortune100/500企業など

- Cloudy with a Chance of Hijacking Forgotten DNS Records Enable Scam Actor (2025/5/20, Infoblox)
  - サブドメインテイクオーバーを起点として攻撃を展開する脅威アクター（Hazy Hawk）に関する報告
    - 被害組織：米国政府系機関、大学、医療系企業・組織、メディア系やその他大企業
  - Hazy Hawkがターゲットにしている（と疑われる）サービス：
    Akamai, **Amazon EC2/S3/Elastic Beanstalk**, **Azure**, **Bunny CDN**, **Cloudflare CDN**, **GitHub**, **Netlify**

NA4Sec
Network Analytics for Security

つなごう。驚きを。幸せを。
docomo Business

参考資料

デジタル庁のドメイン管理ガイドライン改定

- 多発するインシデントを受け、2025/3に改定
- Dangling Record が残らないよう
  削除漏れを注意する内容

２．３　ドメインの移行・廃止方法

ドメインの移行・廃止方法は以下のとおりとするものとする。ドメインの移行・廃止に当たっては、当該ドメインの権威 DNS サーバーに設定された DNS レコード、クラウドサービス等の外部サービスで設定されたカスタムドメインの利用等のための DNS レコードを削除することを含め、意図しない第三者が当該ドメインを利用することを防止する対策を行うものとする。具体的には、DNS レコードの削除では、「CNAME レコード」、「A/AAAA レコード」、「NS レコード」、「MX レコード」等の削除漏れがないよう注意すること、DNS レコード情報の管理者と DNS サーバーの管理者が異なる場合、DNS サーバーの管理者は DNS レコード情報の管理者に対してレコード情報の確認を定期的に依頼し、使用していないドメインの DNS レコードが残存していないか確認することなどを含む。

なお、廃止する Web サイト等について、他の Web サイト等（ソーシャルメディア等の民間サービスを含む）にリンク先等の関連情報を掲載している場合は、運用停止に合わせて~~リンク先~~関連情報の削除を行うものとする。

https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/44df7733-3df2-4e47-bf0b-85c0353c20c7/02fb7b00/20250527_meeting_executive_outline_11.pdf

JPRSの啓発情報

- 日本レジストリサービス（JPRS）がわかりやすい資料を公開してくれています
  - 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 ～
    （Internet Week ショーケース オンライン 2021）
  - 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
  - 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～
    （Interop Tokyo 2025）
  - JPRS用語辞典「Subdomain Takeover（サブドメインテイクオーバー）」
  - JPRS用語辞典「NS Takeover（エヌエステイクオーバー）」