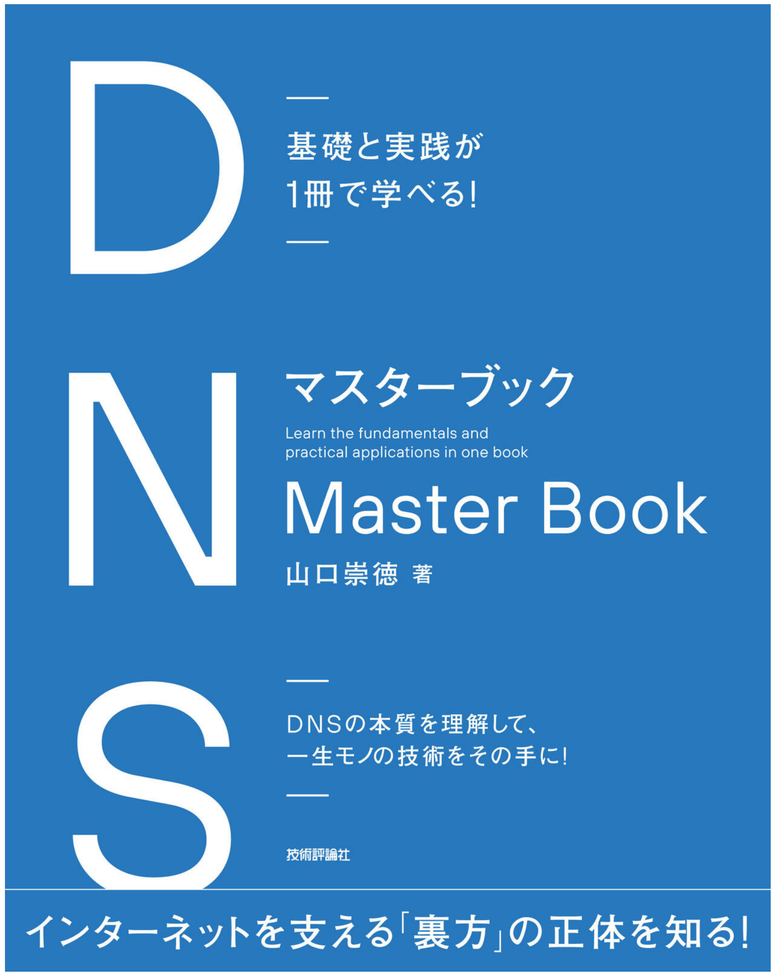
DNSの前に知っておきたい
ドメイン名のセキュリティ

やまぐちたかのり

2026/11/05 JPAAWG 9th

だれだおまえ

- そのへんのおっさん
- 『DNSマスターブック』という本を書きました
  - 今日の資料に含まれる図はこの本からの転載



おしながき

- ドメイン名の登録と管理
- ドロップキャッチ
- まぎらわしいドメイン名
- DNSテイクオーバー

おしながき

- ドメイン名の登録と管理
- ドロップキャッチ
- まぎらわしいドメイン名
- DNSテイクオーバー

ドメイン名とは

https://example.com/hoge
↑これ

From: 何野誰某 <foo@example.co.jp>
↑これ

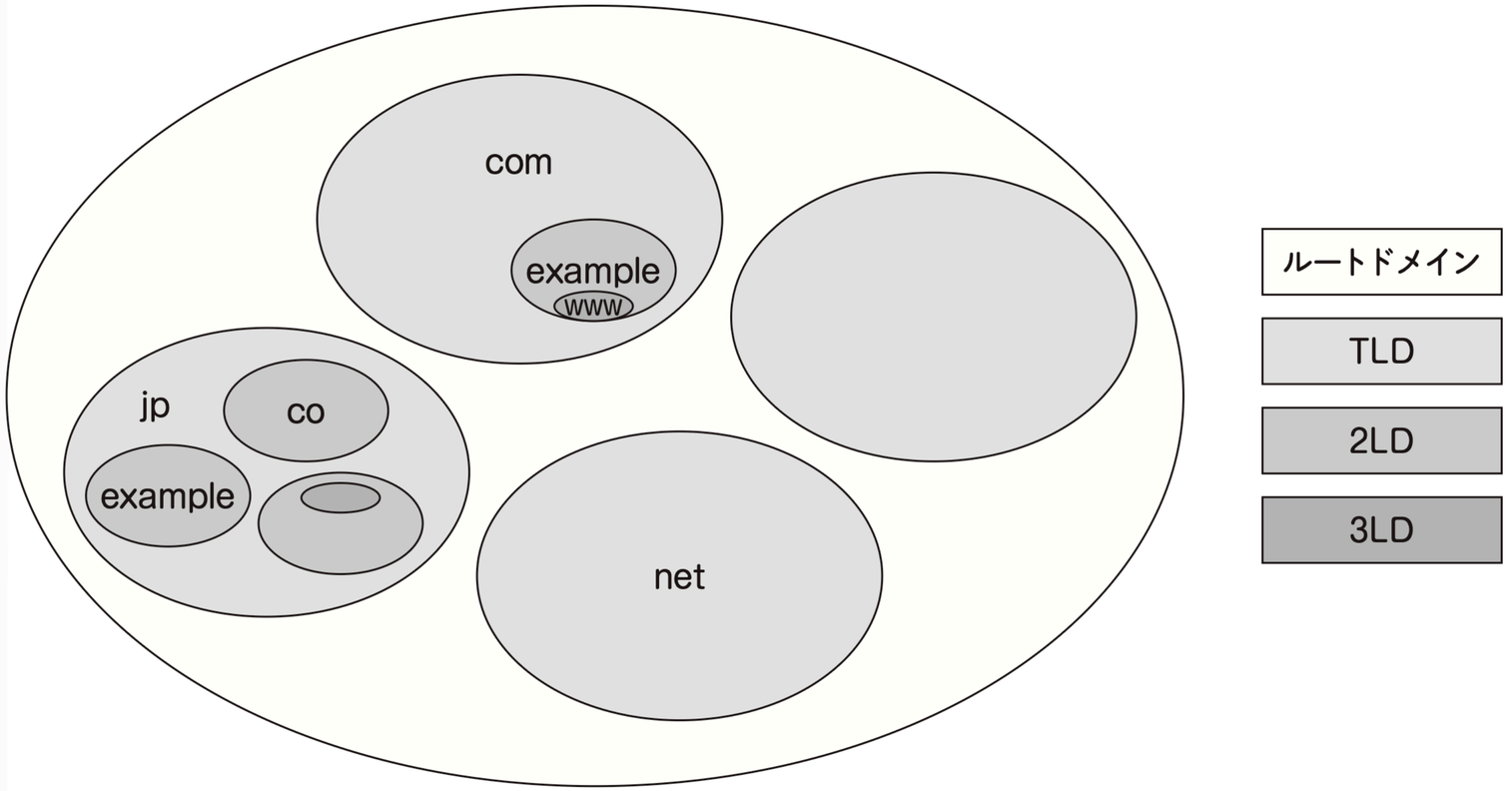
- ドメイン名 ≠ ホスト名
  - https://example.com/hoge の example.com はドメイン名であり、かつホスト名でもある
  - foo@example.co.jp の example.co.jp はドメイン名だが、ホスト名ではない
- ホスト名はホストの名前
- ドメイン名はドメインの名前 → ドメインとは?

ドメインとは

- インターネットにおけるさまざまな資源(リソース)に名前をつけて管理するための入れ物
  - ホストというリソースに名前をつけたのがホスト名
  - ホスト以外のリソース: メール配送先、権威DNSサーバなど
- **階層構造による分散管理**
  - 集中管理では、登録・更新の権限が1ヶ所に集中してしまう
    - インターネット草創期、DNS誕生前は集中管理だった(HOSTS.TXT)
  - それぞれのドメイン管理者が、自分の責任範囲だけを管理する
  - 自分の管理している範囲のうち、一部の管理を他者に任せる

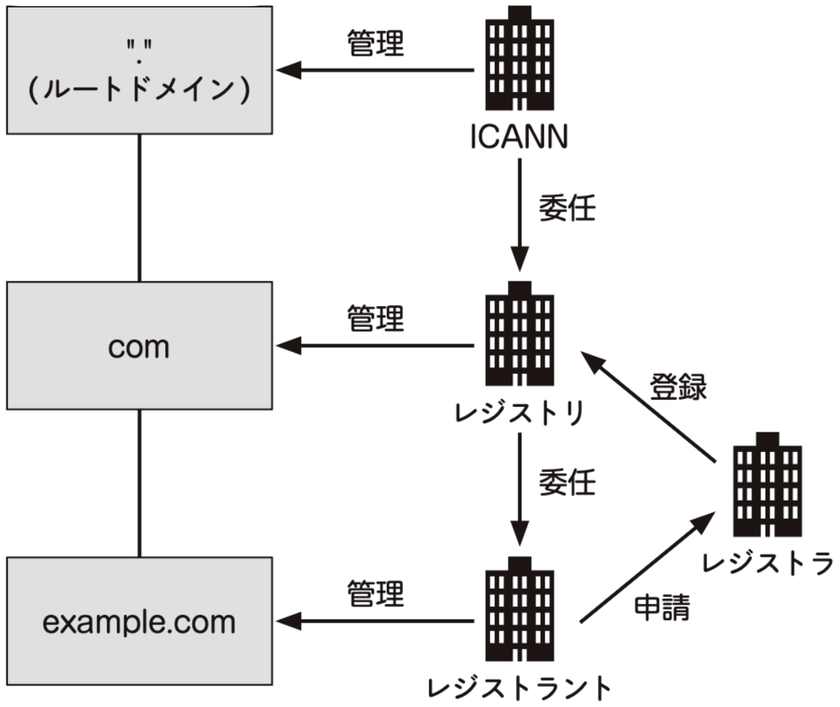
ドメイン名空間

- ドメイン名空間(名前空間): ドメイン名として存在しうる名前全体の集合
- ドメインの一部を分割して権限を委任する
  - 分割したドメインの一部をさらに分割して委任



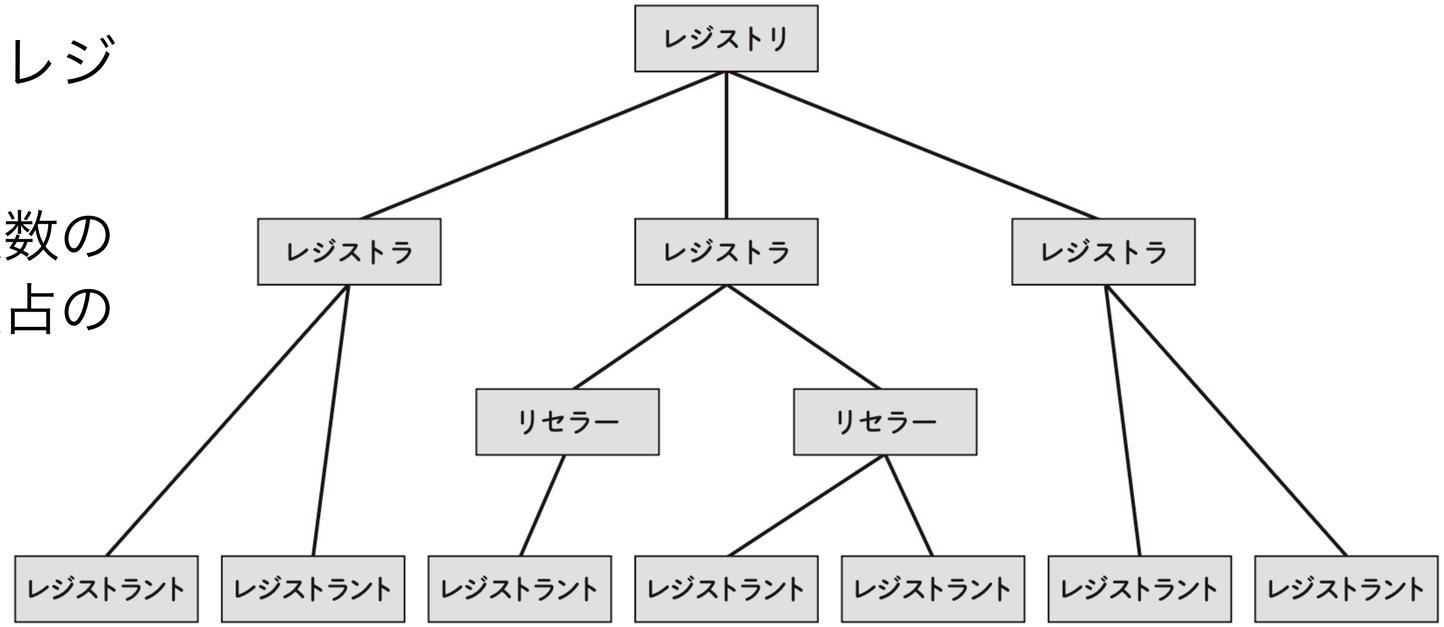
ドメイン名の管理体制(1)

- ICANN: ルートドメインを管理
  - TLDレジストリとの契約、新規gTLDの導入、ルートゾーンの管理などを担当
- レジストリ: TLDを管理
  - 各TLDにつきひとつだけ
    - 同じドメイン名が別の人によって重複登録されないように一元管理されている必要があるため
  - ドメイン名の登録を受け付け、それを権威DNSサーバで公開する役割



ドメイン名の管理体制(2)

- レジストラ: ドメイン名登録事業者
  - レジストラントの要望を受けてレジストリにドメイン名を登録する
  - レジストリは独占事業だが、複数のレジストラが競争することで独占の弊害を減らす
  - jpドメインでは「指定事業者」
- リセラー: 再販事業者
- レジストラント: ドメイン名登録者



gTLD (generic TLD)

- 分野別のTLD
  - gov (米政府)、int (国際組織・政府間組織)など数千
- ただし、分野とは無関係な登録でも認めるgTLDも多い
  - 非営利事業者であっても com (営利組織)に登録できる
  - ネットワーク無関係でも net に登録できる
- 異なるgTLDでも基本的なポリシーは共通
  - 細かな違いはあるが、登録要件さえ満たせばどのgTLDもほとんど同じように使える

ccTLD (country code TLD)

- 国や地域に割り当てられたTLD
  - `jp` など数百
- gTLDとは異なり、ccTLDはポリシーが千差万別
- その国・地域以外の人にも登録を認めるかどうか(**ローカルプレゼンス**)
  - `jp` はローカルプレゼンスが必要
    - 日本国内に住所を持つ個人・法人であることが要件 (日本人でも海外在住なら不可)
  - 外貨獲得などを目的として、ローカルプレゼンス不要で外国人に開放するccTLDも
    - 最近よく見かけるものだと `io` (英領インド洋地域)、`ai` (アンギラ)など

ローカルプレゼンスのポリシー変更

- ローカルプレゼンス不要から必要にポリシー変更されることがある (右表)
  - 既存ドメイン名にも適用されると、これまで使っていたドメイン名を手放さざるを得なくなる
  - 稀な事例だが、jp 以外のccTLDを利用する際には念頭に置く必要あり
- 逆に必要→不要に変更された事例も
  - se (スウェーデン)、my (マレーシア)、sx (シントマールデン)、im (マン島)

ccTLD	時期	備考
ly (リビア)	2010	新規登録かつ3文字以下の2LDのみ適用 (2008年登録の bit.ly は適用対象外)
in (インド)	2026/05(?)	レジストリからの公式発表なし(?) (複数のレジストラが言及しているので導入自体はおそらく事実) 新規だけでなく既存ドメイン名にも適用
ru (ロシア) su (旧ソ連)	2026/09	ロシア政府の認証システムで本人確認できるなら外国人・外国居住でも登録可能 新規だけでなく既存ドメイン名にも適用

ドメイン名の登録情報

- ドメイン名にはさまざまな情報が紐づいている
  - 登録者の名前、住所、その他連絡先
  - 登録日、有効期限
  - 利用する権威DNSサーバの情報
  - など
  - DNSでは利用しない情報も多数含まれる(そっちの方が多い)
- このうちの一部の情報はWHOISやRDAPで誰でも検索できる
  - 公開される範囲はTLDによっても異なる

Web上でのドメイン名管理

- ドメイン名に関する各種情報の登録・更新は、ほとんどの場合レジストラのWeb上でおこなう
- WebUIにログインするための認証情報が漏洩してしまうと、ドメイン名を完全に乗っ取れる
  - DNSSEC (DNSの登録情報を電子署名で保護するしくみ)があっても効果なし
  - なぜなら WebUI から DNSSEC 自体を無効にできるから
- 基本中の基本だが、アカウント情報の管理は厳重に
  - 多要素認証、パスキーなどパスワードだけに頼らないログイン方法で

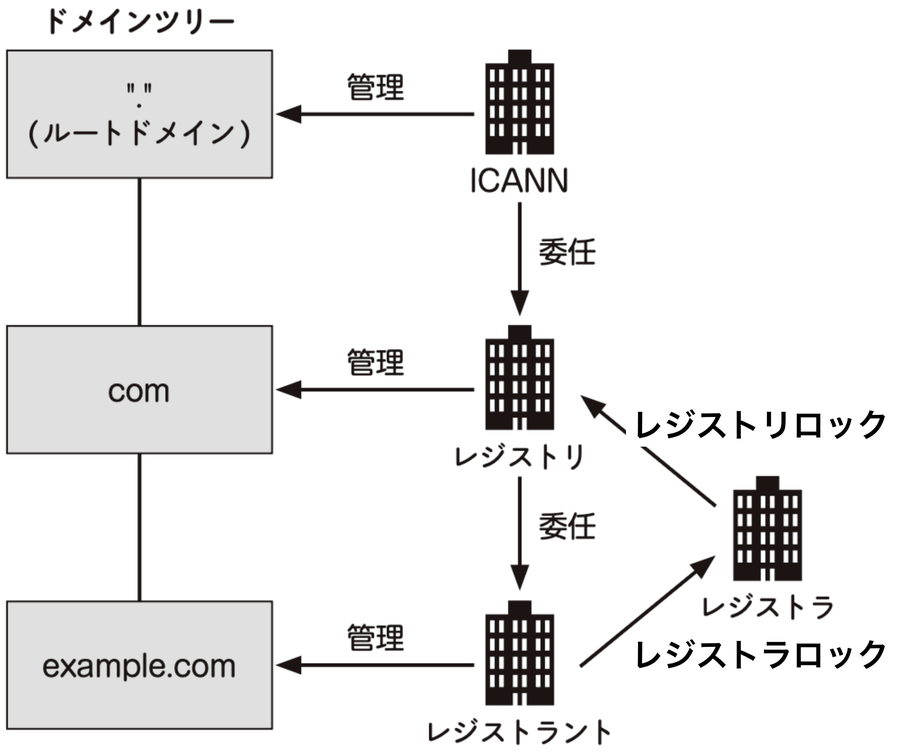
事例: ドメイン名乗っ取り

- 攻撃者がフィッシングサイトとそこに誘導するWeb広告を準備
- フィッシングにひっかかったドメイン名管理者がレジストラの認証情報を入力
- 認証情報を入手した攻撃者はレジストラの管理画面にログインしてドメイン名を別レジストラに移管
- https://blogs.jpcert.or.jp/ja/2023/10/domain-hijacking.html

- 認証情報が漏洩した経緯は不明なものの、同様に移管されてしまったケース
- https://psi.jp/blog/domain_hijacking_2fa

レジストリロックとレジストラロック

- ドメイン名登録情報の意図しない変更を防ぐしくみ
- そのドメイン名に関する登録情報の変更や削除、移管などの申請について、
  - レジストリロック: レジストラからの受け付けを停止する
  - レジストラロック: レジストリへの取り次ぎを停止する
- 必要なときはロックを解除できるが手続きがめんどう
  - 事前に登録しておいた電話番号へのコールバックなど
  - 仮にアカウント情報が漏洩したとしても乗っ取られるリスクは小さくなるが、緊急で変更が必要になった場合への対応も遅れる



おしながき

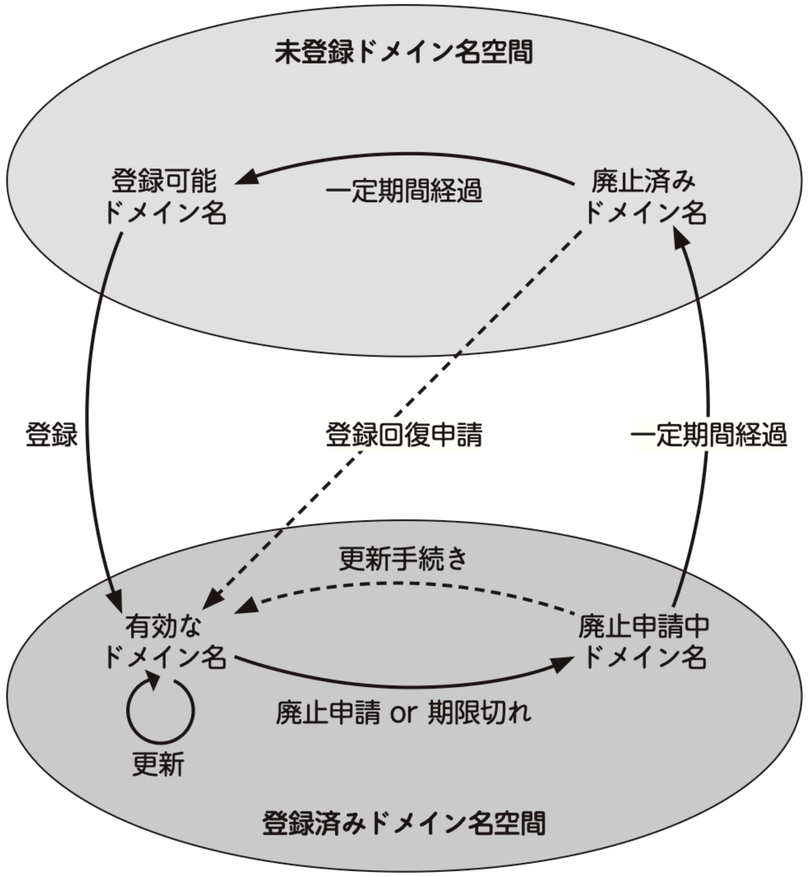
- ドメイン名の登録と管理
- ドロップキャッチ
- まぎらわしいドメイン名
- DNSテイクオーバー

ドメイン名は所有できない

- 一定期間、そのドメイン名を管理する権限を委任してもらうだけ
  - 期間が過ぎれば、更新しないかぎり失効する
- 委任のために必要な情報を**登録**(register)する
  - ドメイン名は「登録」するものであって、「取得」したり「購入」したり「所有」したりするものではない

ドメイン名のライフサイクル

- ドメイン名として使える文字列は無数にあるが、無限ではない
  - IPアドレスやAS番号と同じように、有限の資源
  - ドメイン名もIPアドレスもAS番号も、どれも同じところ(ICANN)が資源管理
- 限りある資源なので、リサイクルされる
  - IPアドレスやAS番号と同じく、**必要なくなって返却されたドメイン名はそれを必要とする別の組織に割り当てられる**



ドメイン名と組織

- ドメイン名はもともと、組織をあらわすものだった
  - ドメイン名 = 組織の識別子
  - メールアドレス = 個人の識別子@組織の識別子
  - 現在も co.jp や ac.jp など属性型JPドメイン名は1組織1ドメインが原則
- **その組織が存続するかぎり長期にわたって使い続けるのが前提**

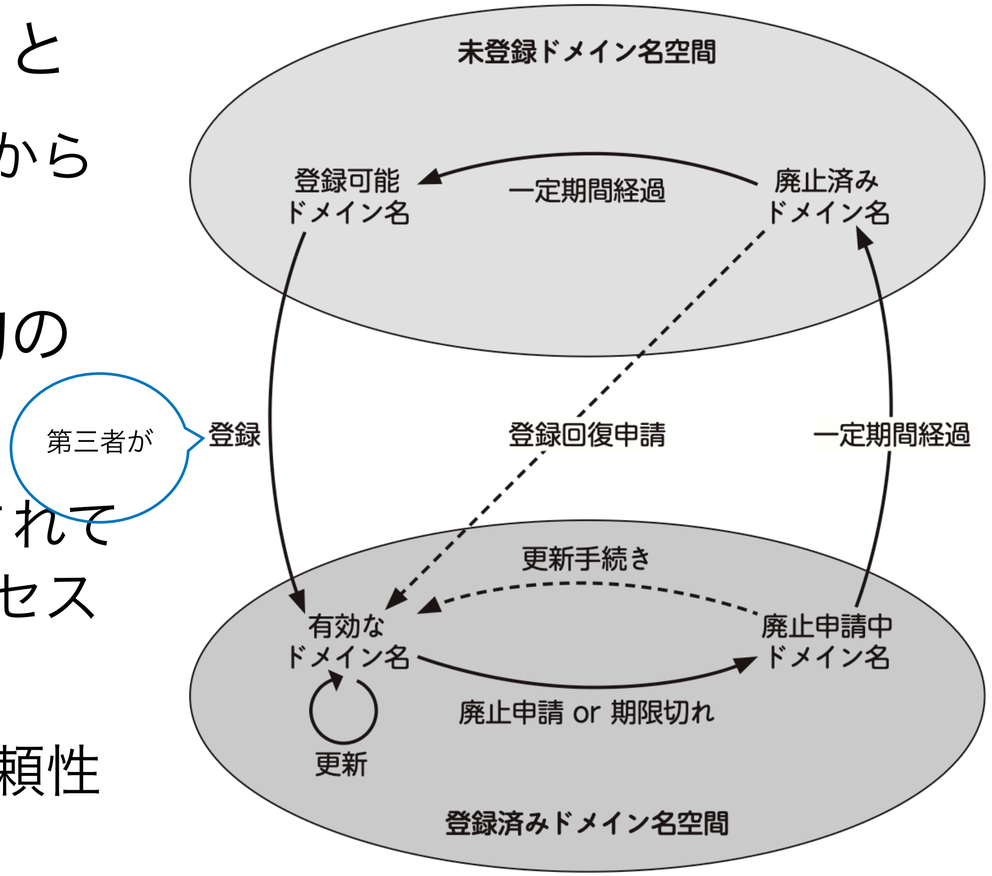
- ……だった

現実のドメイン名

- インターネットの発展にともない、組織をあらわさないドメイン名も一般的に
  - ブランド名、サービス名、イベント、キャンペーン
  - 組織という概念が希薄になり、**短期的利用も多くなる**
  - 組織に紐づかない汎用JPは1組織あたりのドメイン名の数に制限がない
- 実質的にはドメイン名は取得、購入、所有するもの
  - 定期更新は必要だけど
- だが、**廃止されたドメイン名がリサイクルされるという建前は堅持**されている

ドロップキャッチ

- 失効したドメイン名を第三者が再登録すること
  - 廃止されたドメイン名のリサイクルという観点からはルール違反でもなんでもない
- **失効前の知名度・信頼性にタダ乗りする目的**のドロップキャッチが多い
  - 失効前に多くのWebサイトやSNSからリンクされていたドメイン名ならば、容易にそこからのアクセスを獲得できる
  - 公的機関が利用していたドメイン名ならば、信頼性が高いと判断されやすい

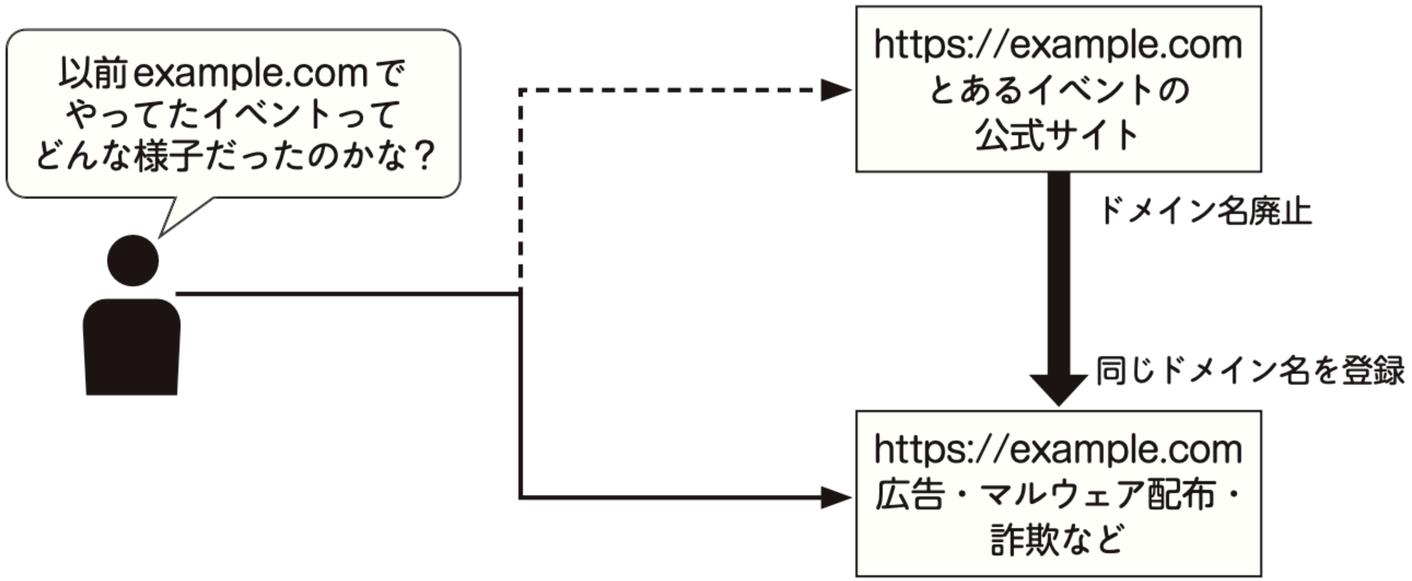


ドメインレピュテーション

- reputation (評判) = ドメイン名の信頼度
  - レピュテーションスコアを提供する事業者がいくつか存在
  - 低スコアのドメイン名はWebフィルタリングや迷惑メール判定の対象になりやすい
  - IPレピュテーションもある
- フィッシングサイト運営者や迷惑メール送信者にとって、レピュテーションスコアの高いドメイン名は価値が高く、ドロップキャッチで狙われやすい
- 逆に、中古ドメイン名と知らずに登録したら以前の登録者がレピュテーションを下げまくっていて、まともな用途でも使いものにならない、という事例も

ドロップキャッチされたドメイン名のその後

- 広告収益を目的とするサイトに化けるぐらいならまだマシなほう
  - マルウェア配布、詐欺、アダルト情報、オンラインカジノへの誘導など
  - アクセスしてきた人に大きな不信感を与えることに



事例: 公的事業用ドメイン名(1)
総合記事

- 自治体が手放した旧ドメインがアダルトサイトやオンラインカジノに…　悪用事例が続々と
  - https://www.chunichi.co.jp/article/1181357
- 公的ドメイン「流出」続出、オークションで高値取引…政府が適正管理呼びかけ
  - https://www.yomiuri.co.jp/national/20240328-OYT1T50139/
- 自治体管理ドメイン悪用が相次ぎ発覚、「使い捨て感覚」脱せずアダルト転用も
  - https://xtech.nikkei.com/atcl/nxt/column/18/00989/120900041/

事例: 公的事業用ドメイン名(2)
新型コロナ関連

- 厚労省公式
  - https://internet.watch.impress.co.jp/docs/yajiuma/1534272.html
- 自治体(ワクチン接種予約サイト)
  - https://www.dnsops.jp/event/20250627/20250627_kakizaki.pdf
- その他関連事業(GoToイート/GoToトラベルなど)
  - https://web.archive.org/web/20231125121653/https://www3.nhk.or.jp/news/html/20231125/k10014268791000.html

事例: 公的事業用ドメイン名(3)
その他

- 大阪・関西万博関連サイト
  - https://piyolog.hatenadiary.jp/entry/2026/08/02/165033
- プレミアムフライデー公式サイト
  - https://www.itmedia.co.jp/news/article/2511/20/1251120093/
- ここで挙げたのは氷山のほんの一角
- もちろん、官だけでなく民で使っていたドメイン名でもドロップキャッチの悪用事例はたくさんある
  - いちいち紹介していたらキリがないので割愛

属性型JPドメイン名も例外ではない

- 属性型JP (co.jp、ac.jp など)は登録のハードルが高い
  - co.jp の場合、会社登記されていることの証明書類が必要
  - が、ちゃんと登記して co.jp をドロップキャッチするケースも珍しくない
  - ne.jp がドロップキャッチされた事例もあり
- 属性型JPドメイン名には仮登録制度がある
  - 法人設立の準備段階(=証明書類なし)でドメイン名を登録できる制度(最大6ヶ月)
  - 実際に法人登記するつもりがなくても、その予定があると嘘をつけば半年限定で co.jp ドメインを使える

事例: スペースワールド

- 2018年に閉園した北九州のテーマパーク
- co.jp だが、少なくとも2回 (もしかするとそれ以上) はドロップキャッチされている
- 直近のドロップキャッチは会社登記のない仮登録



事例: 旧山梨医科大学

- 2002年 山梨医科大学(yamanashi-med.ac.jp)が山梨大学と統合
- 2006年ごろ yamanashi-med.ac.jp を廃止
- 2018年 第三者がドロップキャッチ → 風俗サイトに
  - 指定事業者が登記書類提出前に申請を受理した模様
  - JPRSでの審査も(なぜか)省略されてしまっていた
- ac.jp がドロップキャッチされた事例であると同時に、廃止から10年以上たっていても悪用されるという事例でもある
- https://piyolog.hatenadiary.jp/entry/2019/05/01/102032

ドメイン名の用途はWebだけではない

- ドメイン名はメールでも使われる
- ドロップキャッチした人がメールサーバを稼動させれば、そのドメイン名が廃止されたことを知らずに送られてきたすべてのメールを読むことができる
-

メールアドレスの用途はメールだけではない

- 多くのWebサービスでユーザIDとしても使われる
- 多くのWebサービスではメールを受け取ることができればパスワードを初期化できる
- ∴ メールで使われていたドメイン名をドロップキャッチすればWebサービスのアカウントを乗っ取れる
- Webサービスに登録されていた個人情報やクレカ情報の窃取などのリスク

事例: SNSアカウント乗っ取り

- SNSに登録していたメールアドレスのドメイン名が期限切れでうっかり失効
- 悪意の第三者がドロップキャッチ
  → メールを受信できるようにしてパスワードリセット
  → アカウント乗っ取り成功
  → なりすまし投稿
- https://piyolog.hatenadiary.jp/entry/2019/08/14/065733

対策

- **使い捨て用途のために新規ドメインを登録しない**
  - 既存のドメイン名を活用する
    - https://イベント名.既存ドメイン名
    - https://既存ドメイン名/イベント名/
    - など
- どうしても新規ドメイン名の登録が必要な場合は、**利用終了後も長期にわたって維持できる体制**を構築しておく
  - 担当者の異動による更新メール未確認などを未然に防ぐために、担当者個人ではなく組織として管理する

適切なドメイン名管理

- **ドメイン名の登録・廃止プロセスの整備**
  - あちこちの部署がバラバラに管理するのではなく、統一されたルールで一元管理する
    - ドメイン名管理担当部署を通さないドメイン名登録は禁止する
  - 既存ドメイン名の活用は柔軟に、新規ドメイン名の登録は厳格に
    - 新規ドメイン名のほうが稟議などの手間が少ない、ということのないように
  - 利用終了後も最低でも数年(できれば10年以上)は廃止せず登録を維持できる体制
- ドメイン名の棚卸し
  - その組織で登録・管理しているドメイン名のリスト作成
  - 更新期限のスケジュール管理、利用状況の可視化

ドメイン名は呪いである

- ドメイン名はいまや単なる文字列ではなく、知財と同列に扱われるべきもの
  - それを手放そうとしているうっかり者がいないか見張っている輩が多数いる
- **一度登録したドメイン名は廃止するべきではない**
  - 「ドメイン名は資源であり、必要に応じて再利用される」というお題目を信じても、いまのインターネットでは痛い目を見る可能性が高い
  - 手に入れてしまったら末代まで手放せない、**永遠にコストがかかり続ける負債**の一種

おしながき

- ドメイン名の登録と管理
- ドロップキャッチ
- まぎらわしいドメイン名
- DNSテイクオーバー

URLやメールアドレスの偽装

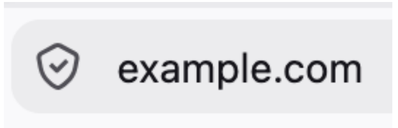
- リンク先URLが表示されたURLと同じとはかぎらない
  - 実際のリンク先URLを確認する必要がある

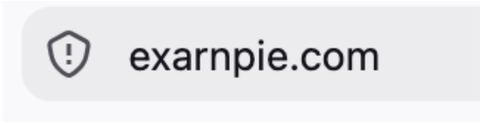
```
From: 何野誰某 <foo@example.co.jp>
```

  - 差出人メールアドレスの偽装は容易
  - 無条件に信頼してはならない
  - SPF、DKIM、DMARC



ホモグラフ(homograph)攻撃

- またはホモグリフ(homoglyph)攻撃
- 見た目の紛らわしい文字を使ったドメイン名で、本物のURLと勘違いした人がアクセスしてくるのを待つ
  - 本物 

偽物 

  - “l”(小文字のエル)と “I”(大文字のアイ)と “1”(数字のイチ)、 “0”(数字のゼロ)と“O”(大文字のオー)、“m”(エム)と“rn”(アール、エヌ)、“w”(ダブリュー)と“vv”(ブイx2)など
  - 国際化ドメイン名(英数字以外を使ったドメイン名)ではまぎらわしい文字が増える
    - “ａ”(キリル文字)、“ο”(ギリシア文字)、“ í ” (アクセント記号つきアルファベット)など
    - 日本語ドメイン名では“口”(カタカナ)/“口” (くち)、“ニ”(カタカナ)/“二”(漢数字)など

タイポスクワッティング

- ドメイン名の入力ミスを狙う攻撃
  - スペルミス、キーボード上でとなりにある文字、ハイフンの有無、単数形/複数形、com なのか co.jp なのか、など
  - 最近は音声入力の誤認を狙ったものもある (for→4など)
- 入力ミスでアクセスした先にあるのは、詐欺サイトやマルウェアだったり
- ドメイン名やURLの直接入力は極力避ける
  - 信頼できるサイトからのリンクをたどったりコピペしたり
  - メールアドレスはアドレス帳から

事例: gmai.com

- gmail にメールを送ろうとしてタイプミスで別ドメインに送って情報漏洩
  - “l”のない gmai.com
  - “a”じゃなくて “e”の gmeil.com
  - など
- 年に数回にはニュースになってる
  - https://xtech.nikkei.com/atcl/nxt/column/18/00676/041700076/
  - https://scan.netsecurity.ne.jp/article/2023/07/26/49726.html
  - 当然ニュースになってない事例も多数あるはず

レベル/コンボスクワッティング

- ドメイン名に example.com が含まれるから OK、とはかぎらない
  - example.com.malicious.invalid のような example.com をサブドメインに含むドメイン名 (レベルスクワッティング)
    - malicious.invalid のサブドメインは example.com の登録者の意向とは無関係に使える
  - login-example.com のような example.com を含む別ドメイン名 (コンボスクワッティング)
    - example.com とは別のドメイン名なので誰でも自由に登録できる
    - example.com の正規のグループ会社がこのような形式のドメイン名を使うこともあり、フィッシングとは一概に判断できないことがある

短縮URLサービスによるフィッシング

- アクセスさせたいURLとは別のURLが表示される
  - まっとうなサイトもフィッシングサイトもURLは https://t.co/xxxxx
  - フィッシングサイト、詐欺サイトへの誘導に使われやすい
- いまどきURLを短縮する必要性は薄い
  - もともとは twitter の文字数制限を回避するために生まれたものだが、現在の X は URLの長さにかかわらず一律23文字でカウント
  - 怪しいサイトや文字数の制限のないところで短縮URLサービスが使われていたらフィッシングを警戒すべき

QRコードによるフィッシング (Quishing)

- そもそも文字列ですらない
  - 正当なものかどうか人間が識別するのは不可能
  - スマホのカメラで表示されるのは URL の一部だけ
    - 実際にアクセスしてみないと正当なものかどうかわからないことがある
- Web上にあるQRコードのうち15%がquishing だったという調査も
  - https://unit42.paloaltonetworks.com/qr-codes-as-attack-vector/
- 警視庁の注意喚起
  - https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/notes/qrcord.html

事例: 短縮URLサービスの詐欺広告

- とあるURLを短縮URLにして、さらにそれをQRコード化
- 利用した短縮URLサービスは、本来のURLにリダイレクトするのではなく Web画面にリンク(+広告)が掲載されるタイプのものだった
  - いっしょに掲載された広告が、フィッシングだった
  - 広告を踏んでしまうとクレカ情報入力画面 (詐欺)
- https://piyolog.hatenadiary.jp/entry/2023/11/12/014635
- QRコードにするなら短縮URLにする必要はない
- 文字数制限がないなら短縮URLにする必要はない

フィッシングに騙されないためには

- 「正しいURL/メールアドレスかどうか慎重に確認する」ことは重要
- が、それで見抜けるケースばかりではない
  - 短縮URLサービスを使うと悪意の有無にかかわらずどのURLも同じドメイン名に
  - QRコード化されるとそもそも文字列として認識できない
- 掲載された媒体の信頼性で判断する
  - 怪しいサイト、怪しいメールに掲載されたURLは踏まない
    - メールが怪しいものかどうかの判断すらせず、ブックマークからアクセスするのも有効
  - 正規の広告ポスターでも、その上に後から貼られたQRコードのステッカーが正規のものとはかぎらない

パスキーの利用

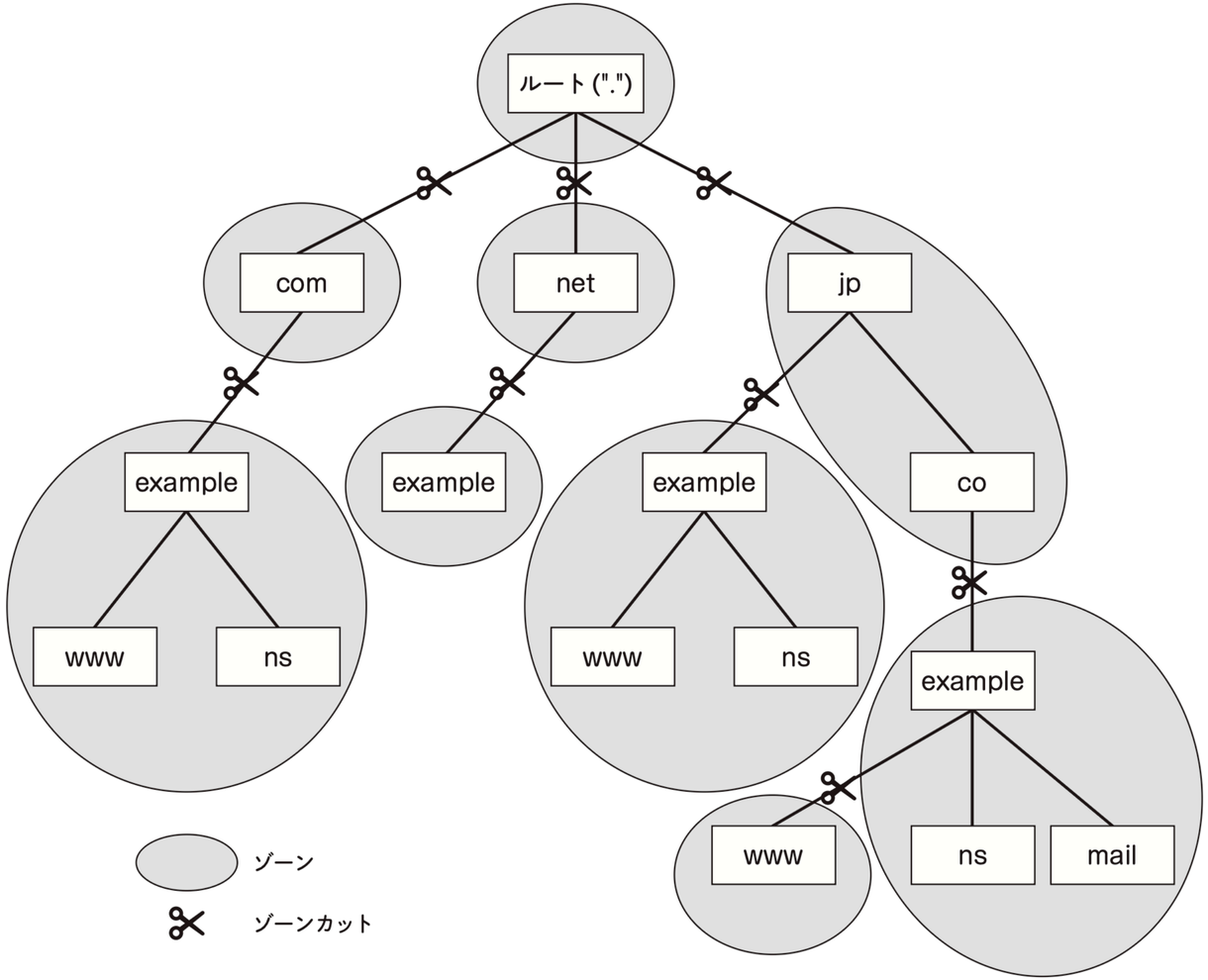
- パスキーの情報はドメイン名ごとに生成される
  - よく似たドメイン名でも、異なるドメイン名なら使い回しされない
  - フィッシングサイトにうっかりアクセスしてしまっても、正規サイトの認証情報が盗まれることがない
- パスキーに対応しているサービスでは積極的に使うようにすべし
- パスキーをクラウドサービスなどで同期する場合、そのクラウドサービスのアカウントを乗っ取られないように十分な注意が必要

おしながき

- ドメイン名の登録と管理
- ドロップキャッチ
- まぎらわしいドメイン名
- DNSテイクオーバー

DNSとは

- ドメイン名をインターネットで扱えるようにするしくみ
- 分散管理
  - ドメインの一部を切り出して、別の人に管理を**委任**する
  - 管理を委任されたドメインの一部をまた切り出して、さらに別の人に委任
  - ゾーン = 分散管理の単位

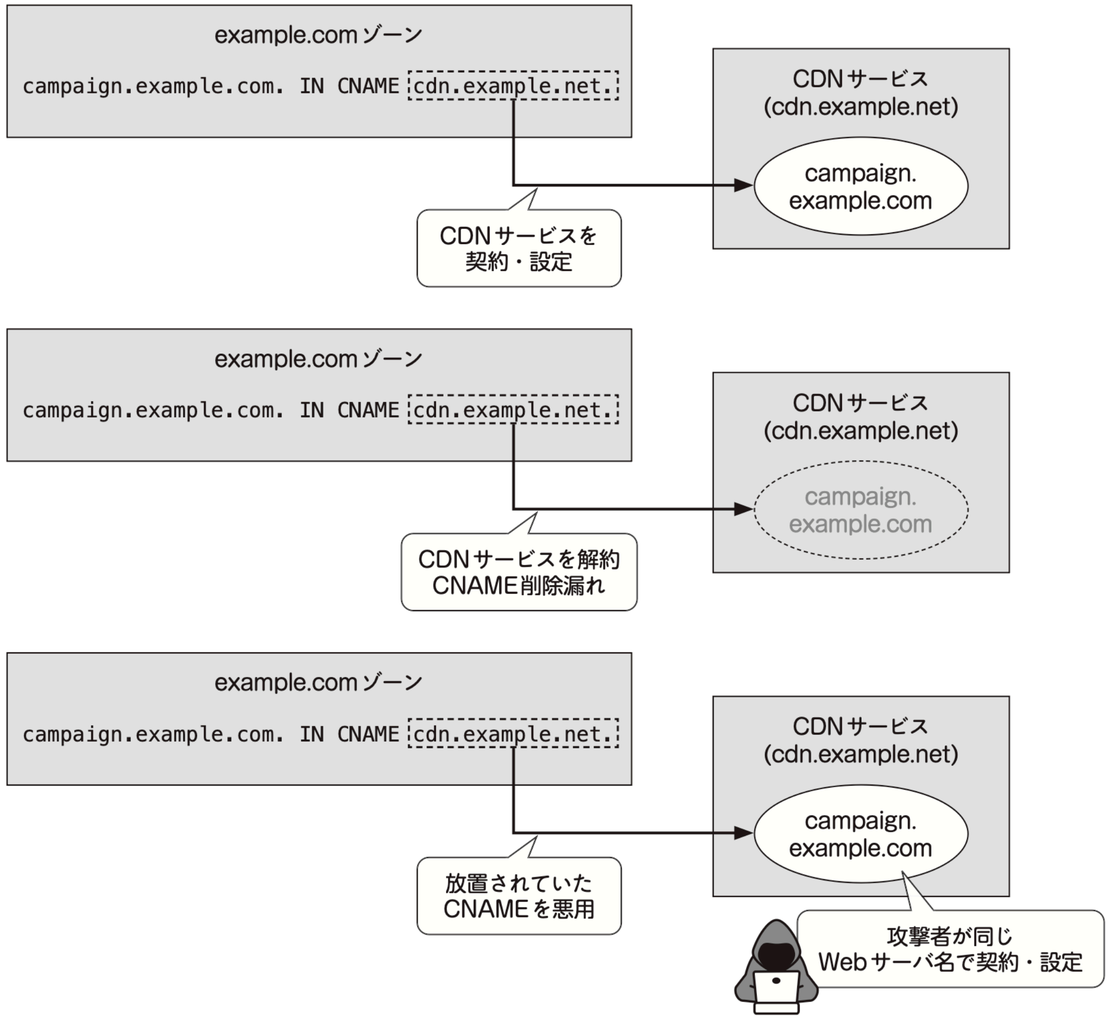


DNSはインターネットの道案内

- DNSはディレクトリサービスの一種
  - 他のディレクトリサービス: LDAP、ActiveDirectory、地図、道路標識など
  - リソースそのものではなく、リソースが「**どこにあるか**」を示すサービス
- リソースを削除するなら、「どこにあるか」の情報も削除する必要がある
  - お店を廃業するときには、お店の場所を案内するための「次の信号右折」の案内看板も撤去しておかないと、そのお店がまだ営業していると勘違いされてしまう
  - 悪意の第三者が居抜きでいかがわしい店を開店して、営業中と勘違いしてやってきた客を騙すかも
  - DNSでも同じことができる

サブドメインテイクオーバー

- campaign.example.com という期間限定キャンペーンサイトを CDN サービスを使って動かす
- キャンペーン終了したら解約
- CDN は解約しても、DNS から削除漏れ
- 同じ CDN サービスで攻撃者が同じ名前の campaign.example.com を契約すると、攻撃者の作ったコンテンツを閲覧できてしまう



DNSテイクオーバー

- 各種の外部サービスを解約した後も、それを利用するための情報がDNSから削除されていないときに、悪意の第三者がそのサービスに同じ名前で契約してアクセスを奪う攻撃
  - CDNだけでなく、メール (MXレコード)や、権威DNS (NSレコード)のアウトソース、SPF (TXTレコード)、各種SaaSサービス(CNAMEレコード)などで同じ攻撃が可能
- 解約したのにDNSから削除されず放置された情報(ダングリングレコード)が悪用される
  - dangling = 宙ぶらりん

DNSテイクオーバー対策

- 「契約がないのにDNSに登録されている」状態を避ける
  - 過去に利用していたサービスでDNSから削除を忘れているものがないか定期的に棚卸しする
- 外部サービスの利用終了後は、宙ぶらりん状態にならないように**先にDNSの情報を削除してからサービスを解約**する
  - 外部サービスの契約前にDNSに登録してしまった場合も同じ攻撃を受ける危険がある
  - サービス契約→ DNS登録 → サービス利用 → DNS削除 → サービス解約という順番を守るべし

事例: go.jp の第三者利用

- 国交省のドメイン名のサブドメインがDNSテイクオーバーで第三者に乗っ取られてオンラインカジノに誘導する広告サイトへ
  - https://xtech.nikkei.com/atcl/nxt/mag/nnw/18/041800012/021700277/
- 悪意の第三者に乗っ取られる前に善意の第三者がテイクオーバーして保護した事例
  - https://www.esd21.jp/esd21dangling/

TLSとドメイン名

- レジストラ管理画面のログイン情報漏洩や、DNSテイクオーバーなどでドメイン名を乗っ取られた場合、乗っ取った攻撃者は正規のTLS証明書を取得できる可能性が高い
  - 前述のDNSテイクオーバー事例も正規のTLS証明書が発行されてしまっている
- 正規のTLS証明書が使われているとエンドユーザは真贋を判断できない
  - 「本物とまぎらわしい偽物」ではなく、「**正真正銘の本物**」が乗っ取られた状態
  - cookieその他の情報がすべて奪われる危険
- HTTPSの安全性が根底からひっくり返る

まとめ

- ドメイン名は単なる文字列ではなく、Web/メール/SaaS/認証その他をつなぐ基盤
- ドメイン名を登録して満足するのではなく、ドメイン名を廃止するまで適切に維持管理し続ける必要がある
  - そのコストを嫌ってうかつに廃止するとドロップキャッチの餌食になる
- 適切なドメイン名管理を!!