

# ドメイン名の事故例／悪用

ドメイン名のライフサイクルマネージメント 2021

2021/11/19

C2 DNS DAY

石田慶樹(DNSOPS.jp)

ドメイン名のライフサイクルマネージメント

ドメイン名のライフサイクルとリスク

インシデント事例

ドメイン名のライフサイクルマネージメント

ドメイン名のライフサイクルとリスク

インシデント事例

# ドメイン名のライフサイクルマネージメント

- ドメイン名の低価格化に伴い使い捨てるの予定でドメイン名を登録
- 組織のポリシーの変更に伴い利用するドメイン名を変更
- 利用終了後に維持料を節約するためにドメイン名を廃止
- ドメイン名を一旦廃止しても一定のリスクが存在
- ドメイン名のライフサイクルマネージメントの重要性

# ドメイン名の登録

- ドメイン名の登録目的
  - 組織指向⇒長期の維持が前提
    - 組織用ドメイン名
    - ブランド用ドメイン名
  - 非組織指向⇒短期的利用が多い(?)
    - サービス用ドメイン名
    - イベント用ドメイン名

# ドメイン名の登録

- なぜ新たなドメイン名の登録を行うのか
- 組織指向ドメイン名のサブドメイン名ではないのか
  - サブドメイン名は分りにくい
  - 組織内で設定・変更するのに時間がかかる
  - SEO対策
  - 組織のポリシーにより困難
    - Webの運用を外部へのアウトソースする場合
    - メール・アドレスの送信先や証明書の組織名の問題

- 使い捨て予定で新たなドメイン名を登録する

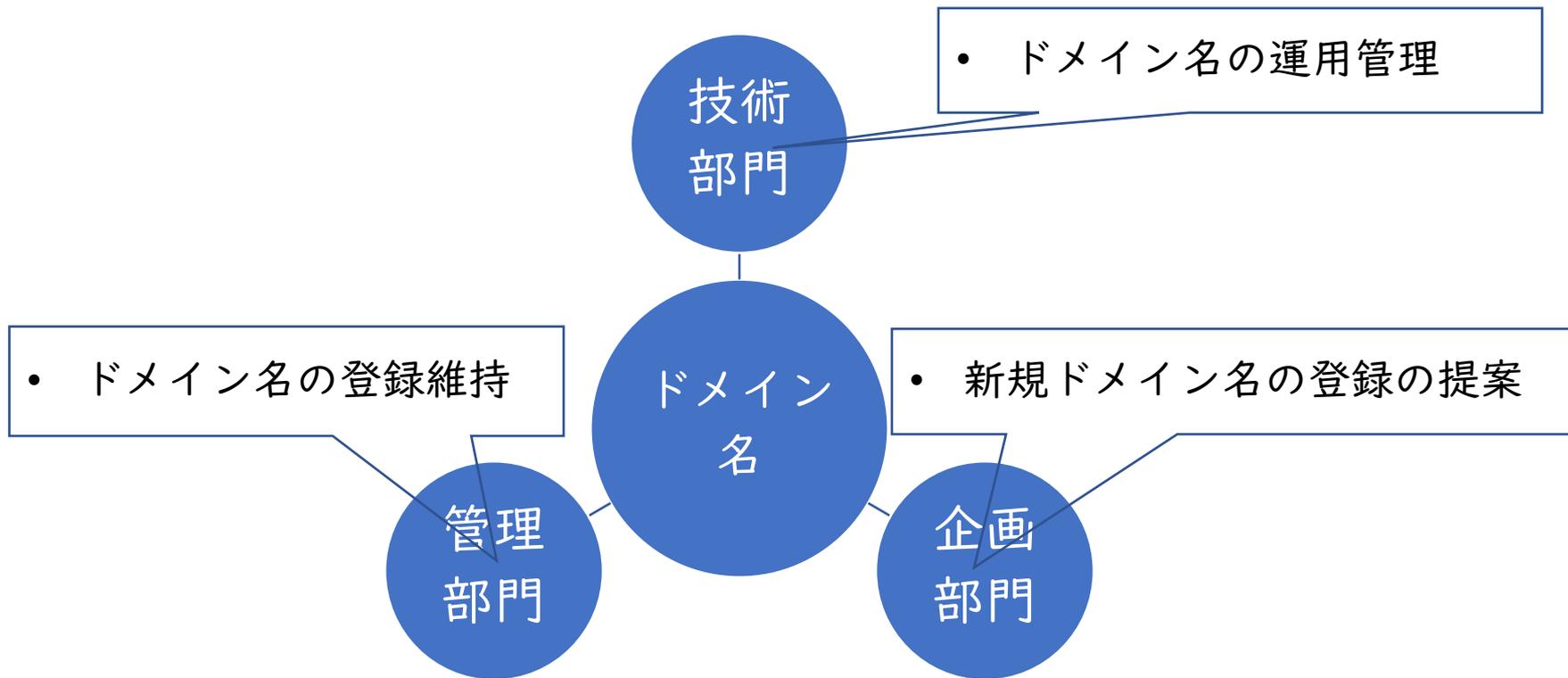


- 利用後にドメイン名を廃止



- ドメイン名の元の登録者が意図しない利用が発生するリスク

# ドメイン名の登録と管理



# ドメイン名の登録と管理 ライフサイクルマネジメント

- 正しい設定と運用
- ライフサイクルの認識
- ドメイン名の運用管理

技術  
部門

- 知財の一部としての管理
- リスクマネジメント
- ドメイン名の登録維持

管理  
部門

ドメイン  
名

- ドメイン名登録の必要性の判断
- 「使い捨て」からの脱却
- 新規ドメイン名の登録の提案

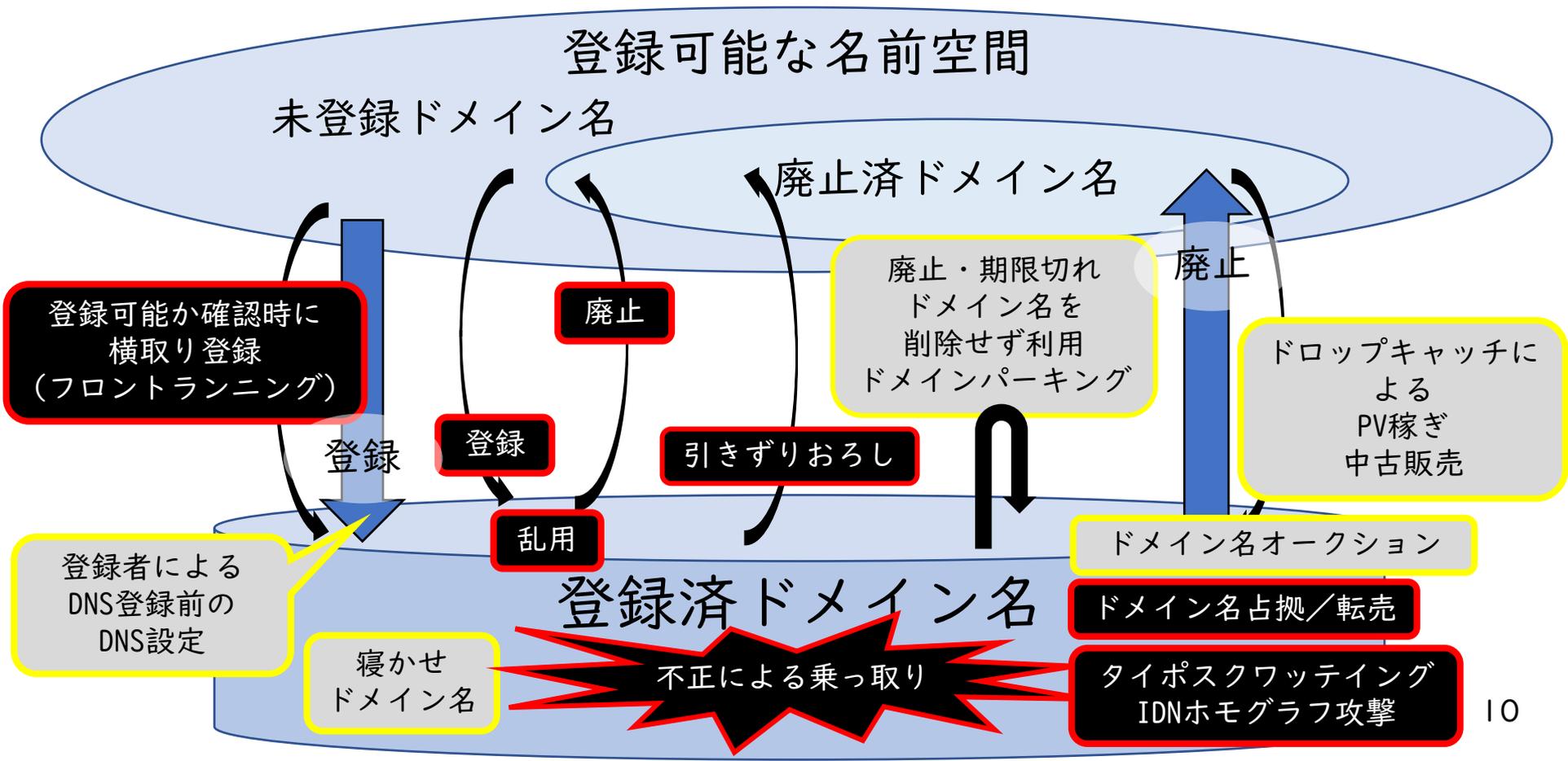
企画  
部門

ドメイン名のライフサイクルマネージメント

ドメイン名のライフサイクルとリスク

インシデント事例

# ドメイン名のライフサイクルとリスク



# ドメイン名に関して発生するリスク

- ドロップキャッチ：  
失効したドメイン名を再登録が可能となるタイミングで第3者が登録すること
- ドメインパーキング：  
使用していないドメイン名を管理するサービス
- ドメインオークション：  
人気のあるドメイン名をオークション形式で購入するサービス
- タイポスクワッティング(URLハイジャッキング/ドッペルゲンガードメイン)：  
有カドメイン名の入カミスしそうなドメイン名により不正なサイトに誘導すること
- IDNホモグラフ攻撃：  
IDNを利用して外見上は同じに見せかけたドメイン名に誘導すること

# ドメイン名のドロップキャッチ

- なぜドロップキャッチが発生するのか
  - 既存のWebサイトが持っているページビューを労せず獲得可能
  - すでに複数のリンクがありかつ検索エンジンに掲載済み
  - SEO対策としてもデメリットが少
  - 一部のドメイン名ビジネスの業者も積極的に加担
  - 専門の業者も存在
- 対策(計画中)
  - ドロップキャッチの実態の把握
  - ドメイン名の利用終了時のサンセットプログラム

# ドメイン名の登録

- Best Practice

- 新たなドメイン名の登録が必要かどうか慎重に検討する
- 登録したドメイン名は価値を高め有効利用する
- サブドメインの利用
  - example2020.jp ではなく 2020.example.jp とする

- ドメイン名登録におけるレピュテーション

- 事業者としてはレジストリ/レジストラ/リセラのいずれも
- TLD そのもののレピュテーション
- 事業者の運用体制のレピュテーション
  - ドメイン名ロックの有無
  - 登録者の認証
  - 登録管理業務のI/F(Web I/F, WebAPI等)
- DNSの運用

ドメイン名のライフサイクルマネージメント

ドメイン名のライフサイクルとリスク

インシデント事例

# ドロップキャッチに関する記事

日経 XTECH

この記事URL: <https://xtech.nikkei.com/atcl/nxt/column/18/00989/12090041/>  
このページに掲載されている記事・写真・図表などの無断転載を禁じます。  
著作権は日経BP、またはその情報提供部に帰属します。  
掲載している情報は、記事執筆時点のもので、変更している場合があります。

打がない

## 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

玄 忠雄 日経クロステック／日経コンピュータ

2020.12.11  
有料会員限定

地方自治体が過去に管理していたドメインが不適切なサイトで利用される悪業が相次いでいる。多くは自治体が期間限定の事業やイベントで使った後に手放し、第三者がこれを再取得して行政とは無関係のサイトに転用しているケースだ。

2020年9～11月に確認できた分だけでも、鳥取県や秋田県大館市、兵庫県神戸市、茨城県が使っていたドメインが中古ドメインを扱う事業者を通じて販売されていた。いずれも売買成立から間もなく不適切なサイトが開発されている。



秋田県大館市が手放したドメインはオークションで第三者が取得したにもかかわらず、市公営サイト（写真）にそのリンクが挿入されたままだった  
（出所：GMOインターネット、大館市、秋田県情報政策連絡協議会）  
（画像のクリックで拡大表示）

- “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” 玄 忠雄 記者  
日経クロステック／日経コンピュータ 2020.12.11
- <https://xtech.nikkei.com/atcl/nxt/column/18/00989/12090041/>

# ドロップキャッチの実例

← ツイート

 **Ryunosuke Sato**  
@tricknotes

このあとの発表資料です!! "クローズしたはずのサービスが知らぬ間に蘇っていたのでクローズしきった話"  
[speakerdeck.com/tricknotes/kur...](https://speakerdeck.com/tricknotes/kur...) #kaigionrails

**クローズしたはずのサービスが  
知らぬ間に蘇っていたので  
クローズしきった話**

2021/10/22  
Kaigi on Rails 2021

Ryunosuke Sato (@tricknotes)

speakerdeck.com  
クローズしたはずのサービスが知らぬ間に蘇っていたのでクローズしきった話  
Kaigi on Rails 2021 での発表資料です。 <https://kaigionrails.org/2021/talks/tricknotes/>

午後5:39 · 2021年10月22日 · Twitter Web App

- <https://twitter.com/tricknotes/status/1451468195743748097>
- <https://speakerdeck.com/tricknotes/kurozusitahazufalsesabisugazhiranujan-nisututeitafalsedekurozusikitutahua>
- ドメイン名をドロップキャッチされて過去のコンテンツのままで公開
- 目的は不明
- コンテンツの不正利用の申し立てによりテイクダウン

# タイポスクワッティングの例

日経 XTECH

この記事URL: <https://xtech.nikkei.com/atcl/nxt/column/18/00676/04170076/>  
このページに掲載されている記事・写真・図表などの無断転載を禁じます。  
著作権は日経BP、またはその情報提供者に帰属します。  
掲載している情報は、記事執筆時点のものです。

勝村幸博の「今日も誰かが狙われる」 [+ 連載をフォロー](#)

## 「gmail.com」へのメール誤送信が相次ぐ、 正体不明ドッペルゲンガーの恐怖

勝村 幸博 日経クロステック / 日経NETWORK 2021.04.21

メールを送ったはずなのに、先方から「届いていない」と言われたことはないだろうか。そのような場合、「ドッペルゲンガードメイン」に誤送信している可能性がある。特に、相手がGmailのアドレスならなおさらだ。ドッペルゲンガードメインの「gmail.com」に吸い込まれている恐れがある。

### 2割以上が「メールの誤送信」

「メールの時代は終わった」などと以前からいわれているが、いまだに使い続けられているメール。多くの企業でビジネスチャットの導入が進んでいるものの、他社への連絡にはメールを使っているところが多いだろう。

そのためメールの誤送信による情報流出が後を絶たない。日本情報経済社会推進協会（JIPDEC）によると、2019年度に報告された個人情報に関する事故（インシデント）のうち、23.2%の590件がメール誤送信だったという。

また日本ネットワークセキュリティ協会（JNSA）によると、2018年中に報道された情報流出に関するインシデントの21.4%がメール経由だったという。

- “「gmail.com」へのメール誤送信が相次ぐ、正体不明ドッペルゲンガーの恐怖” 勝村 幸博 記者  
日経クロステック / 日経  
NETWORK 2021.04.21
- <https://xtech.nikkei.com/atcl/nxt/column/18/00676/04170076/>

# タイポスクワッシングを狙った例



• “東京五輪の裏で起きていたドメイン名取得狂想曲と顛末” 森達哉 早稲田大学教授 2021.10.25

• <https://yab.yomiuri.co.jp/adv/wol/opinion/science/20211025.php>

# IDNホモグラフ攻撃の例

**スラド** 🔍 検索 アカウント作成 ログイン タレコも モバイルページ  
最新 人気 コメント みんなの日記 国民投票 セクション: セキュリティ

## Google Brave.com の偽物 Bravè.com、Googleの広告を通じてマルウェアを配布

ストーリー by nagazou 2021年08月03日 17時05分 巧妙化してるので注意 部門より

headless 日く、  
Google の広告を通じて Brave ブラウザー公式サイト (brave.com) の偽物「bravè.com」への誘導が行われていたそうだ(Ars Technica の記事、 Silent Push のブログ記事、 Braveのセキュリティエンジニア Yan Zhu 氏のツイート)。

偽サイトは Punycode で「xn--brav-yva.com」と表記される国際化ドメイン名 (IDN) だが、ブラウザーのアドレスバーでは「bravè.com」と表示される。このように字形の似た文字を使用したドメインによる攻撃はホモグラフ攻撃などと呼ばれ、以前から行われている。

しかし、今回確認された攻撃では「brave」の Google 検索結果に表示される Brave ブラウザーの偽広告を通じて誘導が行われていたという。広告をクリックすると数回のリダイレクトの末に「bravè.com」へ移動する。brave.com は brave.com に似せて作られており、ダウンロードボタンをクリックするとマルウェアがダウンロードされる仕組みだ。

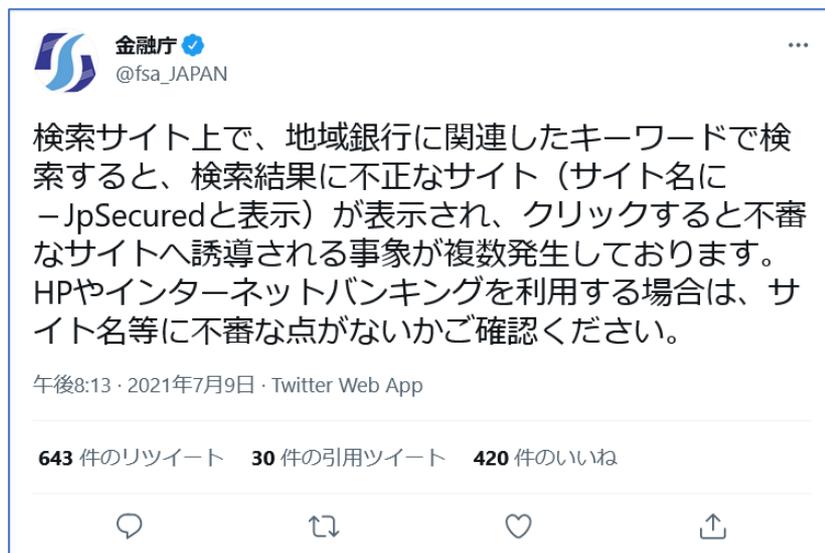
「bravè.com」のほか、「bravè.com」「Exodus.com」「torbrowser.com」「telegram.com」などのドメインが同じレジストラ Namecheap で登録されていたが、指摘を受けて登録は解除されており、Google の広告も既にブロックされているとのこと。なお、現在 Brave ブラウザーで「bravè.com」にアクセスしようとすると、「偽のサイトにアクセスしようとしています」と警告画面が表示される。

3 コメント 🌐 インターネット 🛡️ セキュリティ 📄 広告

🐦 📘 📺 📡

- “Brave.com の偽物 Bravè.com、Googleの広告を通じてマルウェアを配布”
- <https://security.srad.jp/story/21/08/02/1714202/>

# 金融庁が警告したインシデント



- jpsecured[.]com ドメイン名が登録され不審なサイトに誘導
- 目的は不明

# ドメイン名の不正利用への対応

- レジストリ／レジストラに対するガバナンス
  - 日本政府(総務省)によるICANN GACでの訴えかけ
  - ICANN70/ICANN72 の GAC Communiqué に明記
  - 他のステークホルダーも巻き込んだ動きに
  - ドメイン名事業者へのガバナンスの在り方の議論につなげていけるか

# ドメイン名の不正利用

- そもそも論

- ドメイン名関連のステークホルダー(レジストリ/レジストラ/リセラー)はドメイン名の不正利用に対して自覚的にあるべきではないか
  - 機械的な文字列生成による明らかに不正目的の登録
  - 不正利用のためのドメイン名登録
    - SPAM等
    - マルウェア配布
    - 海賊版配布
- 好き勝手にさせることは「インターネットの自由」を自ら毀損することにつながる

# ドメイン名のライフサイクルマネージメント

- ご利用は計画的に

