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

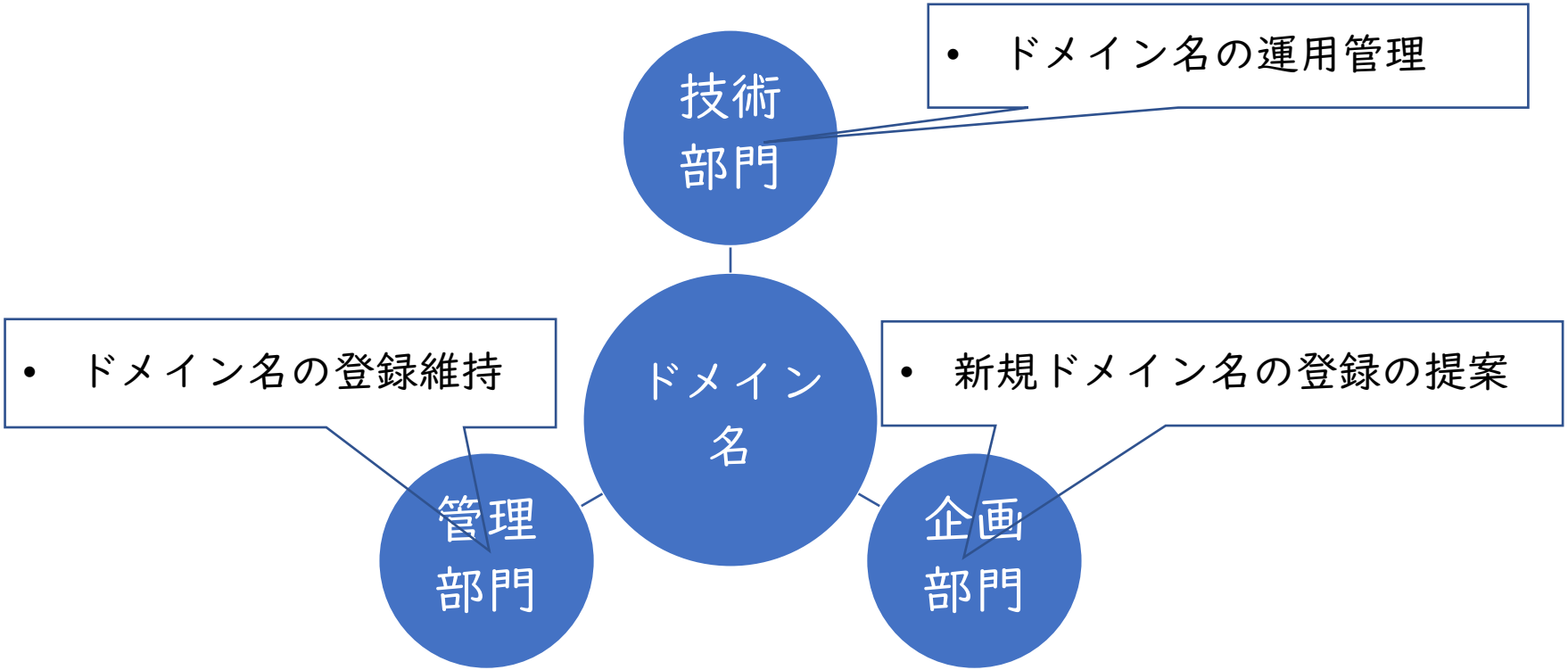
- なぜ新たなドメイン名の登録を行うのか
- 組織指向ドメイン名のサブドメイン名ではないのか
  - サブドメイン名は分りにくい
  - 組織内で設定・変更するのに時間がかかる
  - SEO対策
  - 組織のポリシーにより困難
    - Webの運用を外部へのアウトソースする場合
    - メイル・アドレスの送信先や証明書の組織名の問題

- 使い捨て予定で新たなドメイン名を登録する

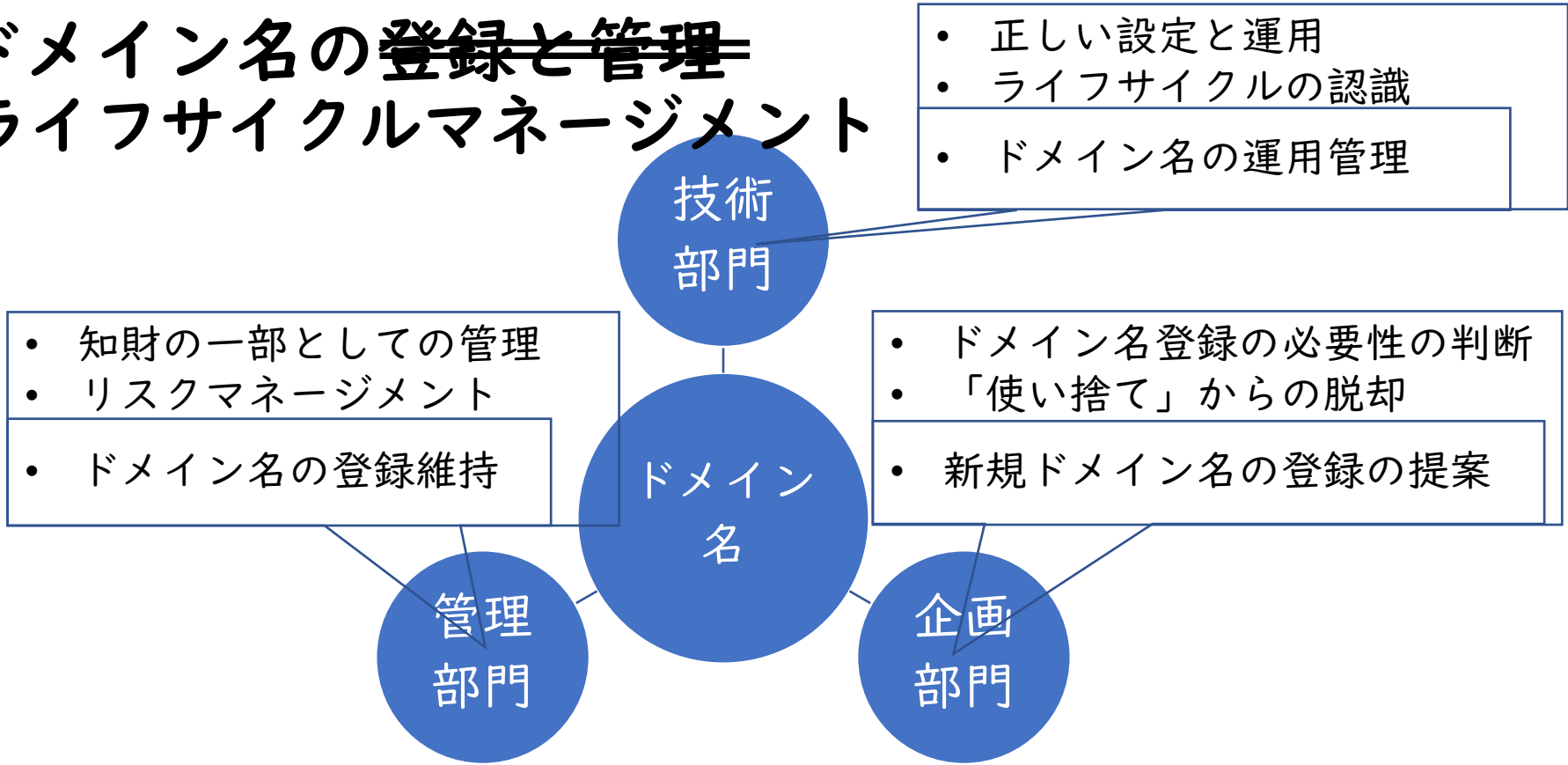
- 利用後にドメイン名を廃止

- 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ージメント

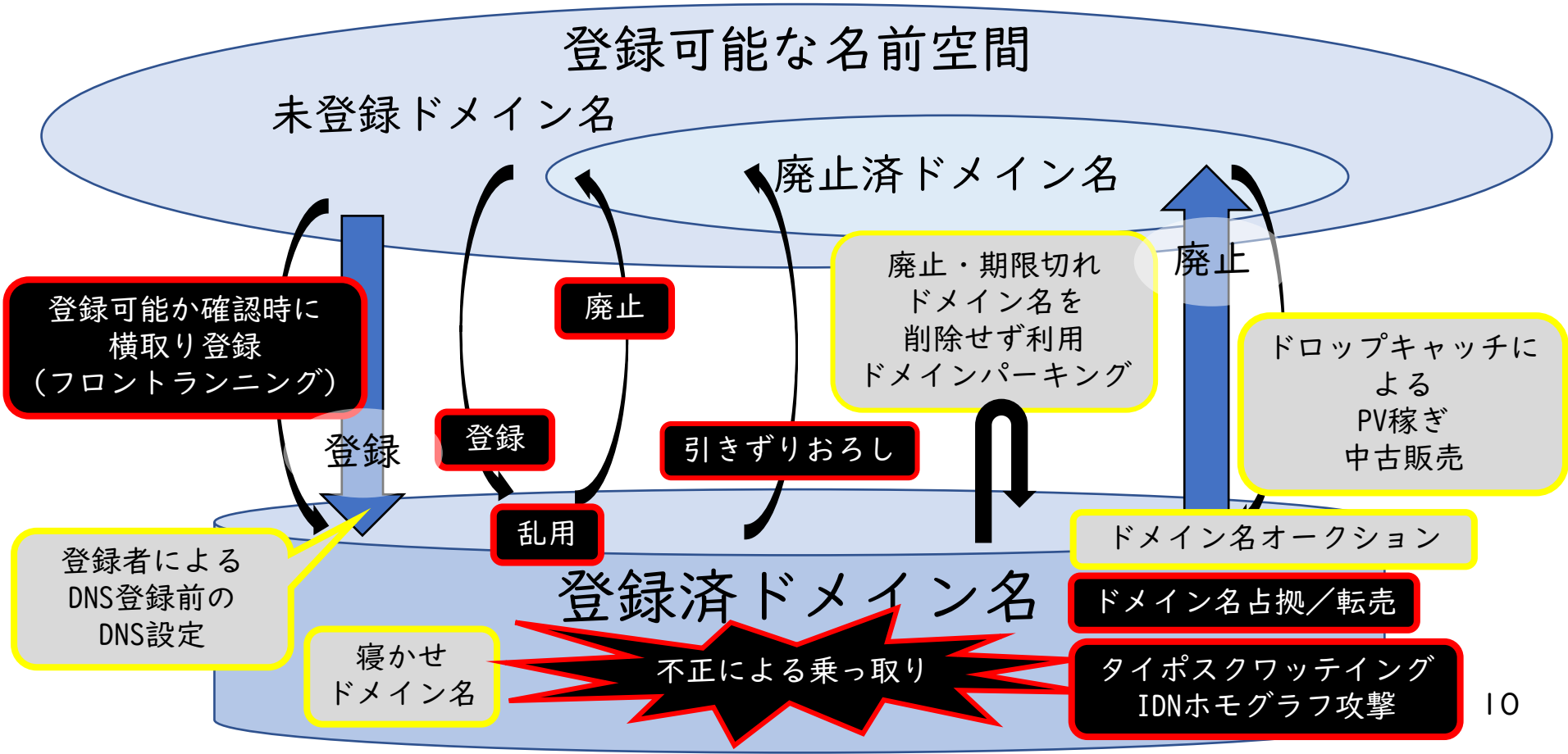


ドメイン名のライフサイクルマネージメント

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)：
  有力ドメイン名の入力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/18/00989/120900041/

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。

IT が危ない　＋ 特集をフォロー

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事案が相次いでいる。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設されている。

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、市公式サイト（写真右）などのリンクは残ったままだった
（出所：GMOインターネット、大館市、秋田県博物館等連絡協議会）
［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/18/00989/120900041/

ドロップキャッチの実例

- https://twitter.com/tricknotes/status/1451468195743748097
- https://speakerdeck.com/tricknotes/kurozusitahazufalsesabisugazhi-ranujian-nisu-tuteitafalsedekurozusikitutahua
- 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/18/00676/041700076/

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

「gmai.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「gmai.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。

- “「gmai.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/18/00676/041700076/

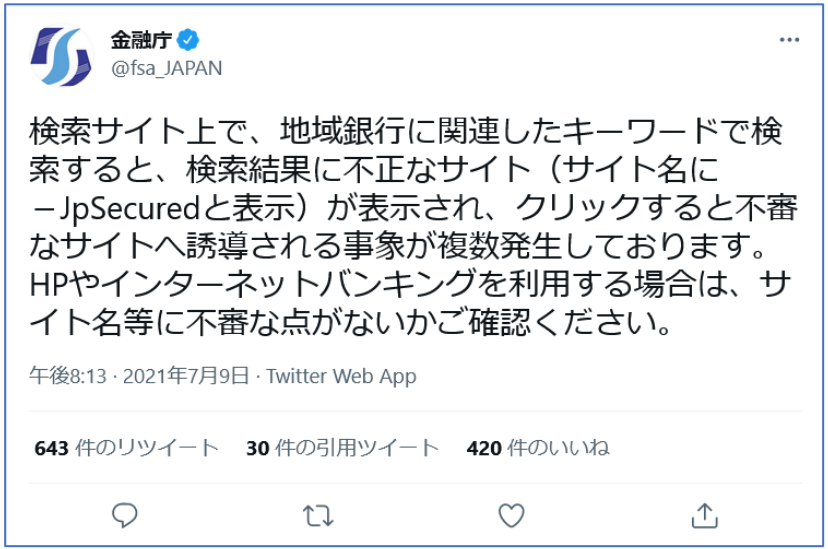
タイポスクワッティングを狙った例

- “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

- “Brave.com の偽物 Bravė.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



金融庁
@fsa_JAPAN

検索サイト上で、地域銀行に関連したキーワードで検索すると、検索結果に不正なサイト（サイト名に－JpSecuredと表示）が表示され、クリックすると不審なサイトへ誘導される事象が複数発生しております。HPやインターネットバンキングを利用する場合は、サイト名等に不審な点がないかご確認ください。

午後8:13 · 2021年7月9日 · Twitter Web App

643 件のリツイート　**30** 件の引用ツイート　**420** 件のいいね

- 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)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