# 合併でわかるドメイン名の管理者

## ～そのドメイン名は誰のもの？～

株式会社JPIX / DNSOPS.JP幹事 白井 出

# 本発表は何を話すか？

## ロ JPNEとJPIXが2023年1月に合併してJPIXになりました。

2023年1月

日本ネットワークイネイブラー株式会社

日本インターネットエクスチェンジ株式会社

合併！

株式会社JPIX

## ロ 本発表では

■合併という一連に作業の中でわかった、ドメイン名登録者とは誰なのかにまつわる曖昧さについて話をしていきます。

# 本発表の動機は何？

## ロ 合併時に気になるドメイン名の周辺事情

### ① 管理者がわからない問題

- 合併時に限らないのですが、混乱状況では誰が管理してるのか？そしてそもそも誰がその存在を知ってるのか？がわからなくなります。

### ② 属性型・地域型JPドメイン名が複数になる問題

- 属性型JPドメイン名には、原則１組織１ドメインという縛りが今でもあります。

### ③ サービス用ドメイン名の移行

- サービスの統合問題なのでDNSOPS.JP範囲外なのですが、実はこれが**今回の本題**です。
  - 範囲外なのになぜここでなのかは後程

# 前振り

JPIX

# ①管理者がわからない問題

## ロ ドメイン名登録状況がわからないのか、誰が管理しているかわからないのか

■ どんなドメイン名登録があるのかわからない。

- 合併時はだいたい混乱します。誰が情報を持っているかわからず困りました。
- 今時は知財部門に情報を集めることもよくあると思いますが、そんな体制がない会社も普通です。
- 金額的に稟議がとられていないケースもあります。古くて稟議が見つからないケースもあります。

■ DNSを自社一括運用していれば、（私たち）DNS運用者ならばドメイン名の登録があることくらいは知っていることが期待されます。

- それでも仮抑えしただけとかNS登録していないドメイン名は存在を知りようがありません。
- また、**権威DNS運用サービス**を使ってる場合など、自社運用していなければ知らないというケースもあります。

■ レジストラも散らばっていたりすると複数社の契約を切り替える必要もあります。

- メールで商号変更を報告しておしまい、のようなところもありましたが、gTLDだとそんなものかもしれません。
- 契約が見つけらないことも想定され、実はまだ切り替わっていない会社が合ってもおかしくありません。
  - もっともお金さえ払われていれば特に問題がないとも言えます。

# ①管理者がわからない問題

## ロ 対処

■基本的には全社管理ドメイン名以外は各システムの担当者に一旦任せました。

- 合併に際し、総務系の部門に情報を集める方針は決定されましたが、道半ばです。

■属性型JPドメイン名のようなケースを除き、**お金が払われていれば**実害はほとんどないため、請求書の管理がキーになるかと思われます。

- 実際、請求書を起因に存在が把握されたドメイン名もあります。
- 過去１年分くらいしか確認できていないため複数年一括払いのものなどは見落としがあるかと思われます。

# ②属性型・地域型JPドメイン名が複数になる問題

## ロ １組織１ドメイン名

■みなさんご存じの通り、属性型・地域型JPドメイン名には１組織１ドメイン名の原則があります。

- 属性が違うものは登録資格を満たせば登録可能ですが、co.jp などは許可されません。
- 昔は、合併に際して移行期間内にシステムを移行しなさいなどというシステム管理者泣かせなことが要求されていました。

■2014年２月頃に状況が変わりました。

- https://jprs.jp/whatsnew/notice/2014/20140217-rule.html
- 端的に言えば、「組織名変更、合併、事業譲渡」時に限り複数のドメイン名を登録・維持することが可能になりました。
  - 新しい組織名で登録することや、既存のドメイン名を両方維持することなどが可能に

# ②属性型・地域型JPドメイン名が複数になる問題

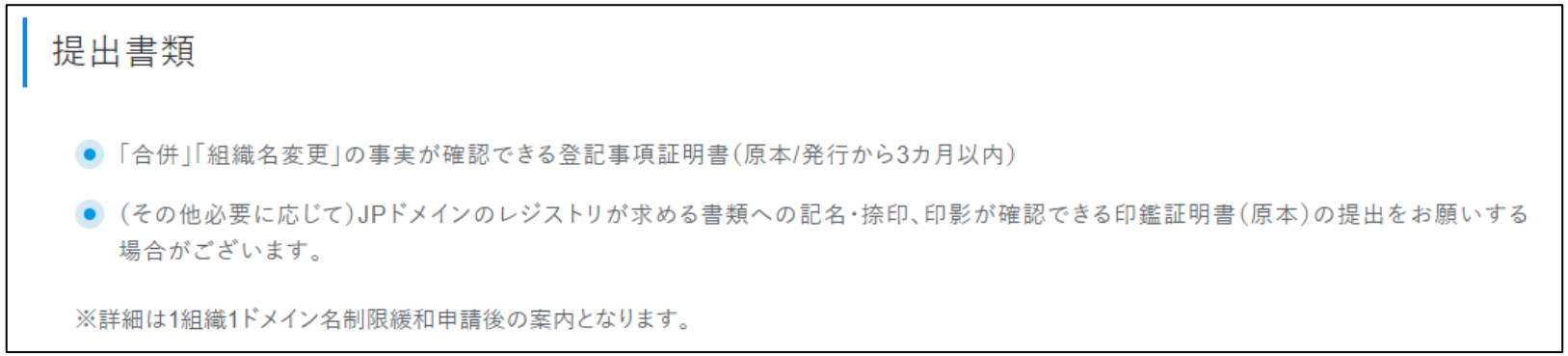
## ロ 緩和申請はどうやるの

■１組織１ドメイン名の制限緩和については、黙っていても大丈夫というわけではなく、緩和申請が必要となります（規約的には下記の書類が必要）。

- ２以上の属性型地域型JPドメイン名の登録依頼書
- 合併、組織名変更または事業譲渡を証する書類

■登録依頼は登録者が直接行うものではなくドメイン管理事業者が行うもの

- このため実際には、「合併、組織名変更または事業譲渡を証する書類」を準備して、ドメイン管理事業者に依頼することになります。
  - 対応していないドメイン管理事業者については移管せよとされていますが、実際にそういう事業者がいるかどうかについては不明です
- 証明に必要な書類




参考：JPDirectの説明 (https://jpdirect.jp/domain/restriction-relaxation/)

# 本日の本題

③サービス用ドメイン名の移行時の問題

JPIX

# ③サービス用ドメイン名の移行

## ロ そこで起きた問題

■直接的には、メールアドレスを @jpix.ad.jp に統合しようとして困ったという話です。

## ロ DNSOPS.JPとどう関係するの？

■各種のサービス利用におけるドメイン名登録者の確認方法に係る問題です。

- 要はドメイン名の管理者は誰なのという問題の一つで、本来の登録者が当該サービスではそのドメイン名を使えなくなるという影響が出ます。

# 前提：一般的にドメイン名登録者の証明って何をするか

## □ 独自ドメイン名を各種サービスで使えるようにするとき

■そのドメイン名の管理権限を持っていることを何らかの手段で確認することにより証明とします。

## □ よく使われる手段

■**DNSの管理・操作権限**を持っていることを証明手段とする。

- ➢ DNSにサービス事業者が指定したTXTレコードなどを追加する方法。

※とてもよく見る証明手段。

■そのドメイン名を使った**システムの管理権限**を持つことを証明手段とする。

- ➢ hostmaster等の特定のメールアドレスへ認証情報を送る方法。
- ➢ Webサーバに認証情報載せたファイルを置く方法。

※簡易的な証明書発行サービスなどで見る証明手段。

■外部の主に**公的情報**を証明手段とする。

- ➢ 法人などで登記情報などを郵送する方法。

※EV証明書発行サービスなどで追加情報として使われることがある。

# 背景：雑な説明

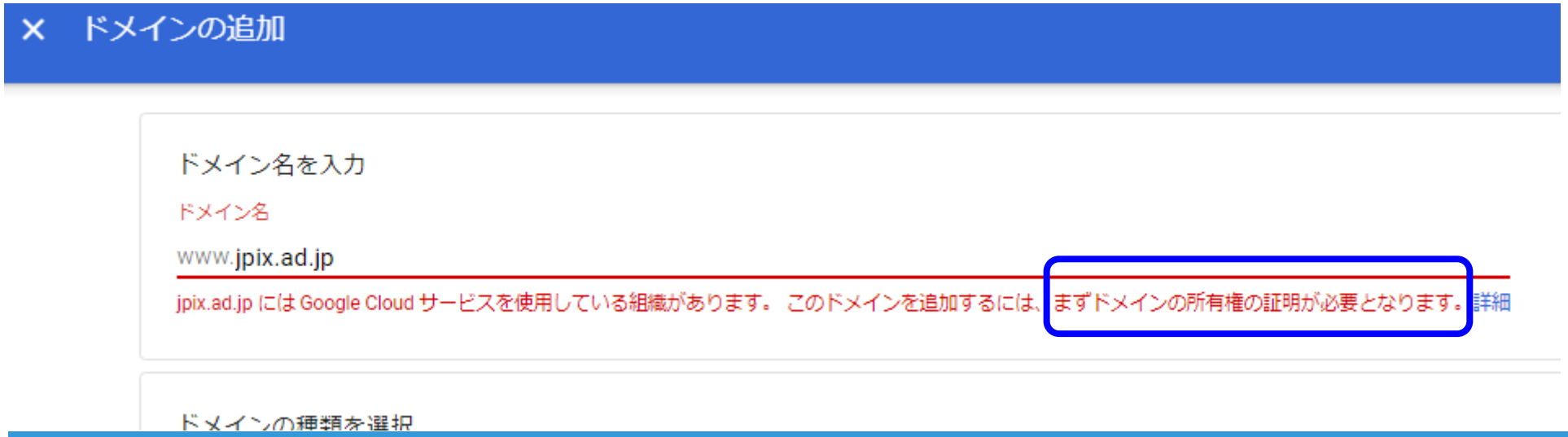
## ロ 社内向けサービス統合が必要

■合併する二つの会社はそれぞれ別のサービスを利用していた

- JPNEはGoogle Workspace
- JPIXはMicrosoft365

■移行過程でGoogle Workspace を jpix.ad.jp をセカンダリドメインに追加したかった

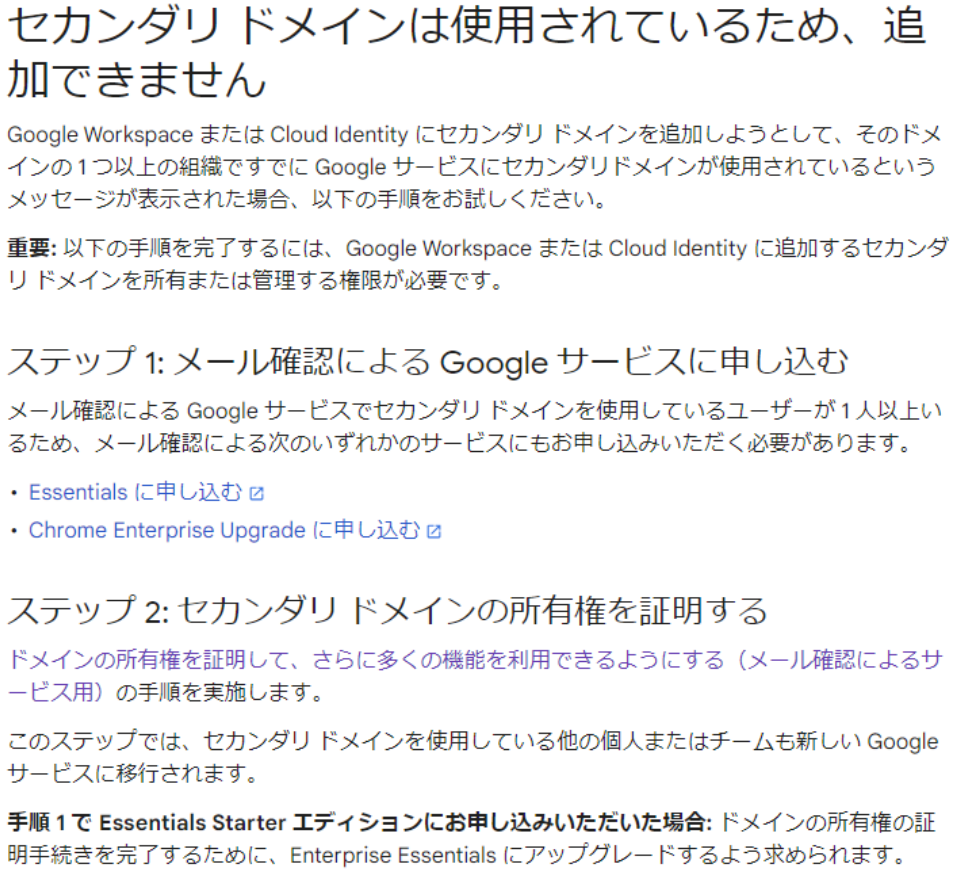
- でも、「ドメインを追加して所有権を証明」（所有権というのは原文ママ）しようとすると、他の人が使ってるからダメだよって言われる



# 背景：誰かが使ってる？所有権の証明？

## ロ 所有権の証明の説明

■https://support.google.com/a/answer/12920197?hl=ja&visit_id=638058814655503956-3297910864&p=add_domain_merge&rd=1#merge_orgs



セカンダリ ドメインは使用されているため、追加できません

Google Workspace または Cloud Identity にセカンダリ ドメインを追加しようとして、そのドメインの 1 つ以上の組織ですでに Google サービスにセカンダリドメインが使用されているというメッセージが表示された場合、以下の手順をお試しください。

**重要:** 以下の手順を完了するには、Google Workspace または Cloud Identity に追加するセカンダリ ドメインを所有または管理する権限が必要です。

ステップ 1: メール確認による Google サービスに申し込む

メール確認による Google サービスでセカンダリ ドメインを使用しているユーザーが 1 人以上いるため、メール確認による次のいずれかのサービスにもお申し込みいただく必要があります。

- Essentials に申し込む
- Chrome Enterprise Upgrade に申し込む

ステップ 2: セカンダリ ドメインの所有権を証明する

ドメインの所有権を証明して、さらに多くの機能を利用できるようにする（メール確認によるサービス用）の手順を実施します。

このステップでは、セカンダリ ドメインを使用している他の個人またはチームも新しい Google サービスに移行されます。

**手順 1 で Essentials Starter エディションにお申し込みいただいた場合:** ドメインの所有権の証明手続きを完了するために、Enterprise Essentials にアップグレードするよう求められます。

「ドメイン名の所有権の証明」として期待していた説明は、前提で示したようにTXTレコードに登録して云々というよくある手段が提示されること

だけど
日本語なのに、正直何を言ってるか全然わからない
なんで使わないサービスに申し込むの？

……
この辺は、Googleのヘルプの問題なんで、
さらっと流して調査に入ります

# 背景：誰が使ってるのか？

## □ 誰かが何かを使っていたのは間違いないらしいので社内聞き取り

■サポートに聞いた感じでは**とりあえず誰かが使っている**という一次回答

■使っているということはどこかに管理者がいるはずで、管理者になるためには先に挙げた手段を使ったはず？

- ➢DNS管理権限で証明。
  - ● DNS管理者に確認するも知らないし更新履歴にもなさそう。
- ➢hostmasterなどのメールで証明。
  - ● 管理者に聞いてもやっぱり知らないし、そもそもGoogle Workspaceにそんな証明手段があるとは聞いていない。
- ➢Webサーバへのファイル配置で証明。
  - ● 同上。
- ➢登記情報などで証明。
  - ● Googleにそんなものを送ったことはない。

結局誰が使っているのかはわからなかった

# 背景：結局どうしたか

## ◘ 管理権限の強制奪取を行った

■https://support.google.com/a/answer/9122284?hl=ja

ドメインの所有権を証明できない場合

ドメインの所有権を証明しようとした際に、次のメッセージが管理コンソールに表示される場合は、管理コンソールでドメインの所有権を証明することはできません。

「他のチームが該当するドメインで Google サービスを使用しているため、ドメインの所有権を証明できません。」

ご利用の Google サブスクリプションでは、同じ Google サービスを使用していない複数のチームの管理をまとめて引き継ぐことはできません。今後のリリースで対応可能になるようアップグレードされる予定です。

他のチームの管理をすぐに始めるには、次のように、他のチームを自身のチームと統合することで、ドメインの所有権を証明します。

1. 他のチームの管理者に、メール確認による Google サービスのサブスクリプションをキャンセルするよう依頼します（手順に進む）。それらの管理者が次のことを確実に行うようにしてください。
   - ユーザーにデータの保持を許可するオプションを選択します。
   - チームの Google サービス アカウントも削除します。

   **他のチームの管理者がわからない場合:** こちらのフォーム を Google Workspace サポートに送信してください。
2. 上記の手順に沿ってドメインの所有権を証明します。
3. こちらの手順 に沿って、他のチームのユーザーを Google サービス アカウントに追加します。

社内利用しかないドメイン名なので強制奪取が可能であったが、利用者が社外にいたら大変だった

強制奪取による影響がヘルプからは全く不明なため、確認に手間取りました。

**他のチーム**の管理者が誰かは教えてもらえない。
というよりサポート窓口ではわからないらしい。

**強制奪取プロセスの流れ**

- DNSへのTXTレコード追加によりプロセスの開始
- 「他のチームの管理者」へGoogleから通知
- 今回は返答がなかったので数日後に強制はく奪
- フリーになったドメイン名をこちらで登録

# 原因調査

## □ とりあえず対処は完了

■やりたかったことはできるようになった

- Google Workspaceでメールを受けたかっただけなんだ…

## □ 誰かが使ってたことの問題

■強制奪取してしまったのでその誰かは何かが使えなくなったはず

- これは社内周知したし「見ざる、聞かざる」

■ドメイン名の登録者が誰も知らないのに何かが使えてしまっていたこと

- 問題はこっち

# 前提：一般的にドメイン名登録者の証明って何をするか　振り返り

## □ 独自ドメイン名を各種サービスで使えるようにするとき

■そのドメイン名の管理権限を持っていることを何らかの手段で確認することにより証明とします。

## □ よく使われる手段

■**DNSの管理・操作権限**を持っていることを証明手段とする。

- ➢DNSにサービス事業者が指定したTXTレコードなどを追加する方法。

※とてもよく見る証明手段。

■そのドメイン名を使った**システムの管理権限**を持つことを証明手段とする。

- ➢hostmaster等の特定のメールアドレスへ認証情報を送る方法。
- ➢Webサーバに認証情報載せたファイルを置く方法。

※簡易的な証明書発行サービスなどで見る証明手段。

■外部の主に**公的情報**を証明手段とする。

- ➢法人などで登記情報などを郵送する方法。

※EV証明書発行サービスなどで追加情報として使われることがある。

**他の手段があったということか？**

# 他の手段があった！

- なんやかんやあって原因は特定
  - ■**Google Workspace Essentials Starter**を使っていた人がいたことが原因
    - ➢これはGmailは使えないがストレージが使えるサービス
  - ■このサービスの識別手段は**個人のメールアドレス**
    - ➢ストレージが使えればよいのだから間違ってもいない
  - ■しかし、このサービスが登録されているとそのドメイン名の管理者がその個人に紐づく
    - ➢それはダメだろう

- ということで原因は、**Google Workspaceのドメイン名検証の仕様**
  - ■…だけならば DNSOPS.JP で話す話ではない

# 当然わいてくる疑問

- 他のサービスでも**他の手段**が採用されているケースはあるのか？
  - ■ドメイン名登録者の確認と個人識別手段があいまいなケースのことですが
  - ■ありました…

**あろうことかOffice365で**

- ■流行ってるんですかね…

| 問題ない | 問題あり |
| --- | --- |
| ドメイン名登録者の証明手段<br>■ DNSへのTXTレコード登録<br>■ 管理者と思しきメールアドレスへメール送付<br>■ 登記簿等の書類利用<br>個人識別手段<br>■ 個人のメールアドレスへメール送付 | ドメイン名登録者の証明手段<br>■ DNSへのTXTレコード登録<br>■ 管理者と思しきメールアドレスへメール送付<br>■ 登記簿等の書類利用<br>■ (new)個人のメールアドレスへメール送付 |

# Office365でのケース

## ロ キーワードはセルフサービスサインアップ

- ■PowerBIとかサインアップするときに出てくるもの。
  - ➢ https://learn.microsoft.com/ja-jp/microsoft-365/admin/misc/self-service-sign-up

## ロ これは、個人の識別としてメールアドレスを使っています

- ■ユニークIDとしてメールアドレスを使うだけですので、これ自体は問題ない。
- ■でも、実はこれそのドメイン名に紐づいた管理者不在のAzureADテナント（セルフサービスサインアップテナント）を作っています。
  - ➢ https://learn.microsoft.com/ja-jp/azure/active-directory/enterprise-users/directory-self-service-signup
  - ➢ 当然、Office365で独自ドメインを使いたいときに既存のAzureADテナントがいるので、Google Workspaceと同様の問題が発生します。
- ■で、こっちの方が問題解決のための操作は大変。
  - ➢ 今回検証まではしていないが机上で確認した範囲では大変そうだった。

# あらためて：ドメイン名登録者の証明手段よく考えると怖い

## ロ 既存の怪しい証明手段の問題

- ■管理者と「思しき」メールアドレスによる証明は適切なのか。
  - ➢「思しき」というのは証明になっているのか？
- ■Web管理者が必ずしもDNSの管理者と連携していない。
  - ➢ 実際JPIXでもWebだけは別管理。
- ■登記情報もよく考えるとドメインの証明は何もしていない…
- ■DNS管理権限の証明（TXTレコード追加）がやはり一番現実的？
  - ➢ それだけに頼るのも怖いが…。

## ロ 上記に加えて新たな問題

- ■個人の証明にメールアドレスを使っているケースで、結果としてそのサービスで本来のドメイン名登録者がドメイン名を利用できなくなることがある。
  - ➢ GoogleとMicrosoftがやってることからレアケースというわけでもなさそうです。
    - ● どちらも漏洩につながるわけではないが…
  - ➢ これは、複数のサービスを統合したプラットフォームを考慮すると不思議ではないと考えられます。
    - ● ドメイン名によるグループ化が機能として組み込まれているが故に、同じプラットフォーム上で個人向けのサービスを提供することにより本来のドメイン登録者の権利を阻害してしまったという問題だと考えられます。

# まとめ

## ロ 合併時はドメイン名という観点でも様々な問題が起きます

■そこでがんばると曖昧だったドメイン名の管理者が整理されます。

## ロ 様々なWebサービスにおいてドメイン名登録者の証明手段は曖昧

■これはよく考えると、昔から曖昧なままとなってきた問題ではありますが、ベストカレントプラクティスとしてDNS管理権限を証明することにより行われてきました。

■一方で、個人がサービスを利用する際の識別情報としてメールアドレスを使うことも当然行われてきています。

■複数のサービスを統合したプラットフォーム上で個人向けのサービスを提供することにより本来のドメイン登録者の権利を阻害するケースがあるということについても考慮が必要です。

# Q&A