技術ホワイトペーパー・提案フレームワーク・バージョン1.0

検知から 対応措置の実施まで

DNS Abuse対応のための測定可能なアーキテクチャ。証拠の来歴、比例的な措置、公的説明責任、迅速な不服申立てを備え、単なる主張ではなく実証試験を前提として設計する。

2026年8月2日公開 | PhishDestroy 研究 | パブリック・コンサルテーション案 | 査読を受けていない

PD-WP-2026-01 · バージョン 1.0 · 2026年8月2日発行
固定URL：https://phishdestroy.io/ja/dns-abuse-enforcement-framework

要旨

独立した提案・ICANNのプログラムではありません

直接的な結論。 gTLDの契約に基づくエコシステムには、ドメインの悪意ある利用が技術的に確認されてから、効果的な対策が講じられるまでに、測定可能なタイムラグが存在します。 公表された研究によると、多くのフィッシングキャンペーンは数時間から数日にわたって継続する一方で、契約上のコンプライアンス手続きには営業日単位の時間を要することが示されています。開示されたシナリオモデルは、遅延がキャンペーンの期待収益をどのように増加させるかを示しています。60～85%という範囲は、本論文における通知後の被害に関する検証可能な中心的な推定値であり、全世界の詐欺全般に関する確立された統計値ではありません。 100～150ドルの技術的見積もりは、定義されたゾーンデータ、Certificate Transparency（CT）データ、およびパブリックフィードデータの収集と一次処理に関するものであり、法的審査や執行にかかる全費用を指すものではない。 本論文では、署名付き証拠、測定可能な対応目標、検証済み事例の自動エスカレーション、状況に応じた是正措置、公的な説明責任、および迅速な不服申立てを提案している。報告者にドメイン停止制御への直接的なアクセス権を与えることは提案していない。

- **一次資料** — 公式文書または公表された研究によって直接裏付けられている。
- **概念モデル** — 市場平均値ではなく、仮定値を入力とする再現可能な計算。
- **政策提言** — 検討、テスト、および修正のために提示されたデザイン。

01 研究課題、研究範囲、および立証基準

この問いは、「誰が失敗したのか？」という問いよりも範囲が狭い：**検証済みの証拠と相応の措置との間に生じる遅延のうち、どの遅延は回避可能か、また、許容できない誤検知や付随的な被害を引き起こすことなく、被害者の被害を軽減できる介入はどれか？**

本報告書の対象範囲は、gTLDの契約に基づくエコシステム、すなわち登録者、再販業者、レジストラ、レジストリ、およびICANNの契約遵守部門です。ホスティングプロバイダー、CDN、ブラウザ、決済サービス、広告プラットフォーム、各国のCERT、および刑事司法当局については、証拠や対応の連鎖に影響を及ぼす場合に限り対象に含まれます。 国別コードTLD（ccTLD）はガバナンスが異なり、ICANNのgTLD契約の対象とはみなされません。

中心的な論点の現状

- 本論文は、ICANNを、gTLDエコシステムにおける民間ガバナンスおよび契約遵守の機関として分析している。ICANNは政府の規制当局や法執行機関ではないが、レジストラの認定を行い、レジストリ運営者と契約を締結し、それらの契約を履行させている。その権限が限定的であるからといって、制度的な説明責任が免除されるわけではない。
- 60～85%という範囲は、本論文の被害モデルにおける中心的な定量的推定値である。これは、明確な仮定や事例の観察結果から導き出された検証可能な推定値として提示されており、世界全体の不正行為全般についてすでに確立された統計値として提示されているわけではない。 検知、通知、被害軽減、および被害発生のタイムスタンプを整合させたインシデントレベルのデータセットを公開することが、次の証拠提示の段階となる。
- 100～150ドルという数値は、汎用インフラ上のアクセス可能なゾーン、Certificate Transparency、およびパブリックフィードのデータについて、継続的な収集と初期選別を行うための、検証可能な技術的予算見積もりです。これは、完全なグローバル可視性、法的審査、異議申し立て、高可用性、あるいは執行にかかるコストではありません。 したがって、本論文では、この数値を、公開済みのワークロード、ソースインベントリ、およびコストログを用いて再現可能なベンチマークとして扱っており、すでに実証済みの普遍的な価格として扱っているわけではない。この区別により、検証対象となっているコストの非対称性を損なうことなく、主張の範囲を絞り込むことができる。
- 本論文における3週間の比較は、コンプライアンスの遅延に関するものであり、ドメイン一斉削除に関する普遍的なSLAに関するものではない。ICANNの 契約遵守に関するよくある質問 同書によれば、ほとんどの苦情の種類については、正式なエスカレーションが行われるまでに、5営業日ずつ3回にわたる対応期間を経ることができる一方、多くの悪意のあるキャンペーンは数時間から数日間も継続して行われるという。契約書では別途、立証可能な証拠が得られた後は、迅速かつ適切な是正措置を講じることを義務付けている。 [2] [4]
- 確認済みの、単一の目的を持つ悪意のある登録については、 `serverHold` これは、ゾーンから委任を削除するため、DNSレベル対策の中でも特に大きな混乱を招くものの一つです。ただし、この対策は万能ではありません。メールやサブドメイン、正当なサービスにも支障をきたす可能性があります。また、TTLが切れるまでキャッシュされた応答が残る場合があり、侵害されたサービスや共有サービスについては、より限定的な対策が必要になる場合があります。 [4] [7]

> **研究への貢献**
>
> この提案は反証可能である。パイロット研究では、トリアージまでの時間、緩和措置までの時間、犠牲者数の代用指標、再発率、偽陽性率、効果の逆転時間、および付随的影響について、介入群と対照群を比較することができる。

02

一次資料が明らかにしていること

$165.1M

ICANN FY27 事業資金

FY27の予算を承認した。これは状況に応じた規模であり、DNS Abuseの支出ではない。 [1]

191,561

2025年のIC3へのフィッシング・なりすましに関する苦情

件数ベースで最大のIC3苦情カテゴリー。直接算定された損害額は2億1,580万ドル。 [10]

24時間

2021年のある研究における生存期間の中央値

1,288件のフィッシングドメインを対象としたデータセット固有の結果であり、普遍的な有効期間を示すものではない。 [11]

SLAは定められていない

一斉削除の期限

2024年の改正では、単一の包括的な期限ではなく、「迅速な」および「適切な」緩和措置が採用されている。 [2] [3]

提案	ステータス	何が言えるか
フィッシングはDNS Abuseである	検証済み	フィッシングは、2024年のgTLD契約改定が対象とする5つのカテゴリーの一つとして明記されている。 [2]
レジストラは行動しなければならない	検証済み	レジストラは、スポンサードネームがDNS Abuseに使用されていることを示す実行可能な証拠を得た場合、速やかに対応しなければならない。 [2]
レジストリは行動しなければならない	検証済み	レジストリ運営者は、実行可能な証拠に基づいて、登録名がDNS Abuseに使用されていると合理的に判断した場合、速やかに対応しなければならない。適切な措置は状況に依存する。 [3]
`serverHold` は委任を解除する	検証済み	これはサーバー側で設定されるEPPステータスである。キャッシュ済みのDNS応答は有効期限まで残る場合があり、この措置は登録ドメイン全体に影響する。 [7]
すべてのDNS AbuseをCZDSまたはCTで把握できる	偽	CZDSとCertificate Transparencyは有用な観測手段だが、すべてのドメイン利用を完全かつリアルタイムに示すものではない。 [8] [9]

ICANNが2024年の改正に基づく契約要件の実施状況について発表した最初の半期報告書によると、192件の調査、2,700件以上のドメイン停止、350件以上のフィッシングページの無効化、および2件の違反通知が記録された。 これらの数字は、現在の管理措置が十分であることを証明するものではないが、システムが何の措置も講じていないという絶対的な主張を否定するものである。 [5]

03

なぜ応答遅延が依然として正当な研究対象であり続けるのか

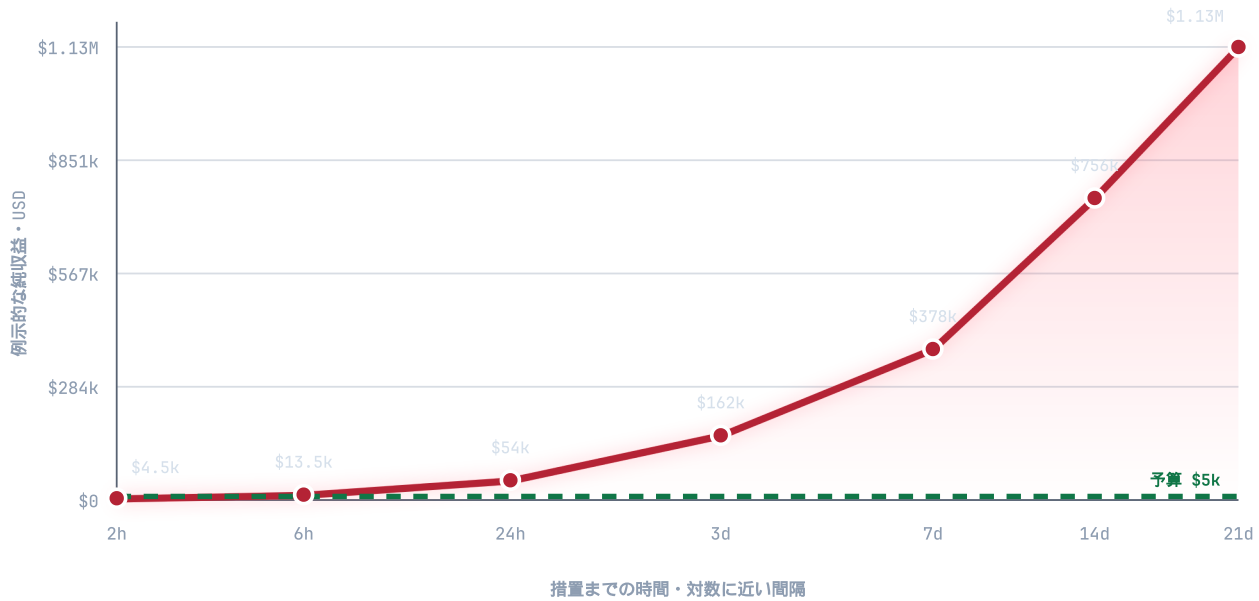
フィッシング攻撃の中には、数時間から数日という時間スケールで活動するものもある。Bijmansらは、2021年に行われたある研究において、1,288件のフィッシングドメインについて、観測された平均存続時間が45時間、中央値が24時間であったと報告している。 [11] 2026年に実施された、新規登録されたフィッシングドメインに関する調査では、その分布に著しい偏りが見られた。存続期間が測定可能な14,112のドメインについて、平均は8.6日、中央値は1日であった。 [12] いずれのサンプルも、あらゆる脅威のカテゴリーに一般化できるわけではありませんが、どちらも、営業日数のみで測定されたプロセスでは、短期間で終了する詐欺やフィッシングの攻撃を見逃してしまう可能性があることを示しています。

測定された時間的ずれ

これらの研究では、通知後に発生する金銭的損害の割合は明らかになっていないが、時間的なミスマッチは明らかになっている。すなわち、初期の非公式な対応段階に最大15営業日を要するプロセスは、平均継続期間が1日程度であるキャンペーンに対するインシデント対応として、それ自体では機能し得ない。 したがって、以下の「21日間」という点は、コンプライアンスの遅延シナリオを示すものであり、普遍的な「ICANN SLA」を表すラベルではない。

図1・詐欺およびフィッシング作戦の累積的な結果を模式的に示したもの

モデル・対数的な時間間隔



この曲線は第4節のシナリオを可視化したものであり、観測された市場データではありません。読みやすさを考慮し、長い間隔は水平方向に圧縮して表示しています。出典：入力が公開されている再現可能なモデル。

因果関係に関する注意

ドメインの存続期間が短ければ、必ずしも金銭的損失が防止されるわけではありません。攻撃者は、検知される前に、別の場所へ移動したり、侵害されたサイトを利用したり、配信経路を変更したり、あるいは資金を引き出したりする可能性があります。因果関係は、サイト閉鎖の速さだけから推測するのではなく、測定する必要があります。

04 再現可能なシナリオとしての詐欺・フィッシング作戦の経済性

経済的に重要な資産は、多くの場合、登録料そのものではなく、ドメインの周りに蓄積されたトラフィック、クリエイティブ、インフラ、そして信頼である。この直感はもっともなものであり、その規模は詐欺やフィッシングの手口によって異なる。したがって、以下の計算ツールでは、観測された平均値として仮定の結果を示すのではなく、すべての入力項目を明示している。

モデルの定義

```
visits(T)   = daily_traffic × T / 24
victims(T)  = visits(T) × conversion_rate
proceeds(T) = victims(T) × average_loss × (1 - cashout_attrition)
profit(T)   = proceeds(T) - campaign_budget
```

シナリオ計算ツール

仮定を任意に変更してください。数値はあくまで例示であり、一般的なフィッシング市場の推定値ではありません。

概念モデル

詐欺・フィッシング作戦の予算（USD）

5000

1日あたりの訪問数

2000

被害者転換率（%）

1.5

被害者1人あたりの平均損失額（USD）

2400

現金化時の減耗率（%）

25

所要時間（時間）

24

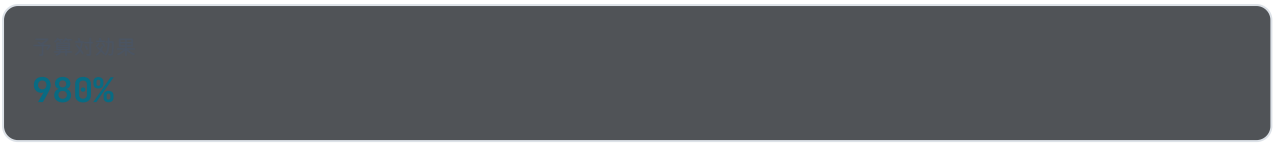
2,000

30

$54,000

$49,000

2.2 h



このモデルは期待値を表すため、予想被害者数は小数になり得る。トラフィックの減衰、検知による行動変化、作戦の移行、被害者の重複、不確実性分布は考慮していない。

▶ モデルのソーステーブルを表示

05 「精度」をでっち上げることなく、予防可能な被害を測定する

「検出後の損失」が有用な成果となるのは、検出、伝達、および被害が一貫して定義されている場合に限られる。ブラックリストのタイムスタンプは、レジストラが法的措置を講じられる証拠を受け取ったことの証明にはならない。ウォレットの取引は、自動的に特定のドメインに帰属するものではない。ドメインにアクセスできなくなったとしても、その変化を引き起こした主体が特定されるわけではない。

イベントスキーマの最小構成

イベント	必須のタイムスタンプ	最小証明
最初の観察	`t_obs`	センサー、リクエスト / レスポンスのハッシュ、キャプチャ方式、クロックソース。
技術的検証	`t_valid`	再現性指標、査読者の身元、脅威のカテゴリー、および信頼度。
通知の送達	`t_notice`	認証済み受領証および証拠書類一式のバージョン。
責任ある当事者は次のように認めている	`t_ack`	ケースIDおよび対象の役割：ホスト、レジストラ、レジストリ、プラットフォーム、または当局。
緩和効果が確認された	`t_mitigate`	DNS、HTTP、決済、またはプラットフォームの状態を、複数の視点から測定します。
不服申立て / 復旧	`t_restore`	決定の根拠、証拠の変更、および復元検証。
ハームイベント	`t_harm`	匿名化された被害者報告、関連付け可能な取引、またはその他の文書化された代替情報。

提案される成果指標

$$\text{Post-notice harm share} = \frac{\text{attributable harm with } t_{harm} > t_{notice}}{\text{all attributable harm in the observation window}}$$

分子と分母には、同じ帰属ルールを適用しなければならない。 結果の報告にあたっては、コホート、信頼区間、右側打ち切り、データ欠損の要因、重複被害者の取り扱い、および観察期間に対する感度について記載する必要があります。「予防可能」というラベルは、因果関係を検討する研究デザイン、あるいは少なくともマッチング比較が行われた場合にのみ使用すべきであり、通知後のすべての事象に適用されるものではありません。

中央値に基づく推定値 · 60～85%

本論文では、モデル化対象のインシデントのカテゴリーにおいて、検出および通知後に発生する帰属可能な被害の割合について、60～85%を中央推定値として採用している。 これは、開示された仮定や事例の観察結果から導き出されたシナリオ推定値であり、世界中のすべての不正行為について測定された統計値ではない。インシデントレベルのデータセットが、観察結果、検証済みの証拠、発生、軽減、および被害のタイムスタンプを整合させるまでは、感度分析に用いるべきである。そのデータセットの公開こそが本論文の立証となるものであり、論文を削除する理由ではない。

06 組織図：能力は分散している

この一連の事象全体を把握し、制御できる単一の主体は存在しません。レジストラは登録者との関係を把握しており、レジストリはレジストリが管理するドメインのステータスを制御し、ホストおよびCDNはコンテンツ配信を制御し、ブラウザやセキュリティベンダーは警告を表示し、決済およびウォレットプロバイダーは送金を中断することができ、当局はデータの保存や差し押さえを命じることができます。ICANNは、gTLDエコシステムにおいて契約を策定・執行しますが、EPPのユニバーサルな制御プレーンを運用しているわけではありません。

01 · SIGNAL

研究者・センサー

コンテンツ、インフラ、被害者に関する指標を観測し、証拠の来歴を保持する。

02 · サービス

ホスト / CDN / プラットフォーム

ドメインを変更することなく、コンテンツを削除したり、アクセス権を迅速に解除したりできる場合が多い。

03 · スポンサー

レジストラ

悪意のある技術的利用を調査し、登録者に連絡を取り、クライアント側のステータスを設定することができます。

04 · ZONE

レジストリ運営者

レジストリで設定されたEPPのステータスおよびTLDゾーンの委任を制御します。

05 · 契約

ICANN コンプライアンス

契約先のコンプライアンス状況を調査するが、すべての不正事件について裁定を行うわけではない。

06 · 法律

CERT / 当局

対応を調整し、管轄区域ごとに定められた法的権限を行使する。

権限の分散は、責任の解消を意味するものではありません。スポンサーレジストラは、不正利用への対応を再販業者に委任したからといって、契約上の義務を免れるわけではありません。レジストリはサーバー設定のEPPステータスを管理し、ICANNは契約の遵守を徹底します。 監査証跡には、誰が行動したかだけでなく、誰が措置を要する証拠を受け取ったか、案件を転送したか、対応を怠ったか、あるいは割り当てられた義務を履行しなかったかも記録されなければなりません。法的権限は、措置を適用する権限を与えられた行為者に留保されます。また、説明責任は、文書化された不履行についても適用されます。

資金の集中と検証可能なインセンティブの相反に関する仮説

$165.1M

2027会計年度　ICANNの運営資金

27年度のベースケース予算を採択した。 [1]

≈98.1%

レジストリおよびレジストラの手数料収入源

1億6,510万ドルの資金調達計画のうち、約1億6,200万ドル。 [1]

70.7%

取引ベースの手数料のみ

$116.8M tied to billable domain transactions. [1]

したがって、資金調達構造は、ICANNが契約の履行を監督する契約当事者からの支払いに大きく依存しており、その大部分は請求対象となる登録取引の件数によって変動する。これにより、構造的な依存関係が生じ、インセンティブの相反という正当な問題が生じている。それは ではない……という事実だけでは、意図的な執行の緩みや「規制の乗っ取り」が成立していることを証明するものではない。この「乗っ取り」仮説は、個々の事案における対応時間、執行の結果、制裁措置、違反の再発、および政策や実施に関する意思決定において資金提供を受けている利害関係者が果たす役割といった要素と照らし合わせて検証されるべきである。

07 2024年の契約上の基準値——そしてそこに明記されていない事項

2024年4月のレジストラ認定契約およびベースレジストリ契約の世界的改定により、DNS Abuseを緩和する明示的な義務が設けられた。レジストラは、スポンサードネームがDNS Abuseに使用されていることを示す実行可能な証拠を得た場合、速やかに対応しなければならない。レジストリ運営者は、実行可能な証拠に基

づいて、登録名がDNS Abuseに使用されていると合理的に判断した場合、速やかに対応しなければならない。いずれの場合も、適切な措置は状況、深刻度、付随的損害に依存する。 [2] [3]

よく混同されがちな3つのタイムライン

年表	適用対象	それが意味しないこと
24時間	RAA §3.18.3に基づき、法執行機関、消費者保護機関、準政府機関またはこれらに類する機関が専用連絡先に提出した、十分な根拠のある違法行為の報告を審査すること。	これは、一律に24時間という停止期限ではありません。
「速やかに」	適用される「措置を講じるべき証拠」の基準値に達した後、適切な緩和措置を講じる。	これは決まった時間数というわけではなく、すべてのケースで同じ対処法が必要というわけではありません。
21日間	正式な契約上の契約違反通知の後、是正期間として設定される場合がある。	これは、報告されたすべての悪意のあるドメインに付与される通常の有効期間とは異なります。

この柔軟性には利点がある。すなわち、侵害された大学のドメインは、新規に登録された単一目的のフィッシングドメインと同じように扱うべきではない。説明責任に関する問題点は、公開されたタイムスタンプ、事案の分類、および結果コードがなければ、「迅速」と「適切」を比較することが困難であるという点にある。以下の提案は、すべての事案に単一の期限が適用できるかのように装うことなく、測定と検証の仕組みを追加するものである。

08 境界の問題：フィッシングは対象に含まれるが、一部の金融詐欺は対象外となる可能性がある

フィッシングは、DNS Abuseの契約上の定義に明示的に含まれる。より難しい境界は、特定可能な第三者を装うのではなく、独自の名称で利用者を欺くサイトにある。例えば、偽の投資プラットフォーム、詐欺的な店舗、返金詐欺、ウォレット署名スキームなどである。事実関係によっては、これらは契約上のDNS Abuseではなく、ウェブサイトコンテンツ上の不正、消費者詐欺、または別の法的カテゴリーとして扱われ得る。

> 研究ラベル案
>
> **検証済み金融被害型不正利用（VFHA）**：ブランドのなりすましの有無を問わず、欺罔によって資金、決済認証情報、秘密鍵、またはシードフレーズを取得するためにドメインが使用されたことを文書化したもの。VFHAは現行のICANN用語ではなく、それ自体で契約上の権限を生じさせない。

政策協議では、VFHAのように厳密な証拠要件を伴うカテゴリーを、将来の契約、分野横断的な照会枠組み、または国内法のいずれに位置付けるべきかを検討できる。範囲拡大には、明確な被害基準、信頼できる証拠、比例的な救済措置、管轄権審査、不服申立てが必要である。曖昧な「詐欺」ラベルだけでは不十分である。

09

月額100～150ドルの監視サービスに関する主張が証明すべきこと——そして証明できないこと

汎用サーバーは、gTLDに参加しているゾーンファイルの公開スナップショットをダウンロードしてローカルで変更点を計算し、選択されたCertificate Transparencyイベントや公開フィードを取り込み、文字列を正規化し、ハッシュを計算し、候補の優先順位を付けることができます。これは有用で検証可能なエンジニアリングベンチマークであり、「インターネットの完全な監視」ではありません。 2026年第2四半期、VerisignはすべてのTLDにわたって4億160万件の登録を報告しました。CZDSはすべてのTLDではなく、参加しているgTLDゾーンファイルを対象としており、CTはすべてのアクティブなドメインや有害なドメインではなく、公開ログに記録された証明書またはプレ証明書を記録するものです。 [8] [9] [17]

機能	汎用プロトタイプ	本番運用の公益サービス
ゾーン / CT / フィードの取り込み	定義済み情報源について実行可能	冗長コレクター、情報源契約、欠測監視
文字列 / ハッシュの選別	実行可能	ベンチマーク、ドリフト検出、偽陰性研究
ブラウザレンダリング	小規模な標本部分集合	隔離実行基盤、地域別観測点、マルウェア封じ込め
法的判断	対象外	有資格審査者、管轄権・権限の対応付け
高可用性 / 証拠保全	通常は未実装	HSM支援署名、監査ログ、バックアップ、インシデント対応
不服申立てと復旧	対象外	24時間365日運用、独立したエスカレーション、サービス目標

図2・桁数の目安 対数幅・同種比較ではないコスト

収集および一次選別段階・年次 $1.2k–$1.8k

強靭なインフラのシナリオ・年次 $10.4k

フルスタッフ体制のプログラムシナリオ・年次 $500.4k

ICANN 2027会計年度の運営資金・年間 $165.1M

対数スケールにより、小さな数値も視認しやすくなっています。 最初の3つの数値は、公表されたベンチマークを必要とする、公開済みの技術的またはプログラム上の仮定であり、ベンダーの見積もりではありません。ICANN 運用資金は、検証済みの機関規模の数値です。これらは意図的に等価ではない予算です。この比較は、基本的な収集と選別が本質的に法外なコストとなるかどうかを検証するものであり、完全な施行プログラムのコストが月額100ドルであるかどうかを検証するものではありません。

10 提案する検証済みDNS Abuse対応フレームワーク

提案されているフレームワークは、自動的なグローバル・キルスイッチではなく、リファレンス・アーキテクチャである。これは、事案の概要、決定記録、およびタイムスタンプを標準化すると同時に、権限を持つオペレーターが、混乱を最小限に抑えつつ効果的な措置を選択できるようにするものである。

01 · 取り込み

取得・保存

レポートや観察結果を収集し、未加工の証拠品を精査し、時計を同期させる。

02 · 証拠の出所・取扱履歴

証拠を標準化する

由来、手法、取り扱い履歴、およびソースの依存関係を記録する。

03 · 検証

裏付ける

有害な行動を再現し、独立した証拠を見極める。

04 · 評価

リスクおよび担保

悪意のある登録、侵害されたサービス、共有ホスティング、および重大度を分類する。

05 · 返信

通知と影響の軽減

担当者を割り当て、目標時期を定め、混乱を最小限に抑えつつ効果的な是正措置を講じる。

06 · レビュー

監査と不服申立て

成果に関するメタデータを公開し、その影響を測定し、迅速な是正を支援する。

証拠のレベル

E1 未確認の信号

単発の投稿、語句の一致、あるいは評判に関する主張。観察対象としては適しているが、これだけでは利用停止の根拠としては決して不十分である。

E2 再現された挙動

認証情報の盗用、マルウェアの配信、または不正な取引経路を示す、タイムスタンプ付きのキャプチャ。

E3 独立した裏付け

少なくとも2つの真に独立した情報源、あるいは再現可能な技術的証明1つに加え、所有権および文脈の確認。

E4

適格な確認

権限、影響を受けたサービス、ブランド所有者、または被害者であることを裏付ける証拠、およびプライバシーを保護した証拠の保管経路。

独立の原則

同一の上流ブラックリストを複製する3つのフィードは、3つではなく1つの情報源である。証拠の来歴グラフは、共通の起点、同期、ベンダーによる再公開を明示しなければならない。

11 最小限の証拠エンベロープと相互運用可能なAPI

APIは、検証可能なケースを作成し、監査可能な対応タイマーを開始する必要があります。報告者は、保留コマンドを直接発行できないようにしなければなりません。E3/E4のケースが単一目的の悪意ある登録に関するものであり、合理的な決定や効果的な是正措置が講じられることなく期限切れとなった場合、システムは自動的にそのケースをレジストリ運営者、または契約上もしくは法的な権限を有する他の関係者にエスカレーションします。A `serverHold` コマンドは、権限を持つ主体からのみ発行される。有効期限切れ時の自動エスカレーションおよびレジストリ操作権限は、提案されているポリシー変更であり、既存の権限に関する主張ではない。すべての状態遷移には署名が行われ、監査ログに記録される。

POST /V1/CASES · 例

```
{
  "indicator": {"type": "domain", "value": "example.invalid"},
  "alleged_category": "credential_phishing",
  "observed_at": "2026-08-02T06:14:22Z",
  "evidence": [
    {
      "type": "http_capture",
      "sha256": "a3f1c9…",
      "collection_method": "isolated_browser_v2",
      "source_id": "reporter:ed25519:7c2a…"
    }
  ],
  "provenance_graph": "ipfs-or-object-store:sha256:91bd…",
  "collateral_context": {
    "registered_domain_scope": true,
    "shared_service": false,
    "mail_observed": true,
    "suspected_compromise": false
  },
  "requested_action": "review",
  "reporter_signature": "ed25519:…"
}
```

応答が成功した場合、ケースID、受信アクター、証拠レベル、完全性に関するエラー、目標レビュー期間、および公開用透明性URLが返されます。管轄権および付随的な影響について、権限のあるアクターが評価を行うまでは、具体的な是正措置を約束してはなりません。

12 提案されているのは対応目標であり、一律の削除期限ではない

サービスレベルの目標は、以下のように区分すべきである *謝辞*, *トリアージ*, *決定* そして *効果的な緩和策*. これにより、サスペンションが常に正しい結果であるとは仮定することなく、パフォーマンスを測定できるようになります。

事例概要	謝辞	トリアージ対象	決定対象	代表的な回答選択肢
単一目的の悪意ある登録におけるE3/E4支払い認証情報またはシードフレーズの盗難	15分	1時間	4時間	コンテンツブロック、許可された場合におけるレジストラ / レジストリによる保留、ブラウザおよび決済に関する警告。
E3ブランドを悪用したフィッシングやマルウェアの配布	30分	2時間	6時間	ホスト / CDNの削除、ドメインへの対策、コントロールポイントに基づくシンクホールまたは警告。
侵害された正規のドメインまたは共有SaaSテナント	1時間	4時間	12時間	パス / アカウントの分離と所有者の復旧；可能な限り、登録ドメインの停止を回避する。
分類をめぐる金融詐欺	4時間	12時間	24時間	保全措置、プラットフォーム / 決済に関する介入、当局への照会、および理由を明示した決定。
E1信号または不完全なレポート	自動車	24時間	検証されるまではなし	状況を監視し、情報を充実させ、証拠の提出を求める。

これらは暫定的な目標値です。正しい値は、観測された脅威の存続期間、人員配置、エラーコスト、および法的制約に基づいて導き出され、単一の平均値ではなく、達成度分布とともに公表されるべきです。

13 安全性、適正手続き、プライバシー、および故障モード

安全対策なしに迅速に対応すると、不正確なデータが検閲、商業的妨害、あるいはインフラの停止へとエスカレートする恐れがあります。したがって、適切なアーキテクチャでは、誤検知や付随的な被害を、最優先のセキュリティ上の失敗として扱う必要があります。

故障モード	必須の制御	監査可能な指標
競合他社に対する悪意のある通報	記者の認証、情報源の信頼性、独立した再現性、および悪意のある技術的利用に対する制裁	報告者別の報告却下率；操作が確認された事例
合意を装ったフィードの循環性	証拠の来歴グラフと上流情報源の重複排除	系統補正前後の独立ソース数
不正利用された正規ドメインを一括停止	登録意向の分類とパスレベルの緩和策の選好	侵害されたドメインのシェア；影響を受けた正規のサービス
被害者の情報や攻撃手法の詳細が公に流出した	段階的な開示、情報の黒塗り、証拠の封印、および保存期間の制限	個人情報漏洩事案；情報黒塗り処理の審査結果
不当な行為が続いている	24時間365日対応の不服申立て受付、独立した審査員、および認証済みの復旧プロセス	中央値および95パーセンタイルの反転時間
レジストリの保留により、メールおよびサブドメインが利用不能に	担保物件の目録、救済措置の比例性、および措置実施後のモニタリング	アクションごとのサービス中断件数；ロールバック率

適正手続きの最低限の保障

1. 制限措置については、その都度、理由コード、証拠の信頼度レベル、および責任ある意思決定者が記録されます。
2. 登録者は、プライバシーを保護した理由説明書を入手し、反証を提出することができます。
3. 緊急案件（不服申立て）は、当初の決定を下した者とは別の担当者が審査を行います。
4. 取り消しは、元の操作と同じ符号付きチャネルを通じて伝播します。
5. エラーおよび復旧に関する集計統計は公開されていますが、機密性の高い証拠については引き続きアクセス制御が適用されています。

14 「毒性スコア」から、説明責任のある「対応品質指数」へ

レジストラの公開スコアは説明責任の向上に寄与するものの、単純なランキングは、ポートフォリオの規模、フィードの網羅性、顧客構成、およびドメインが悪意を持って登録されたか、あるいは後に乗っ取られたかといった要因によって歪められてしまう。スコアを理由に、あるレジストラの全顧客を一括してブロックするようなことは決してあってはならない。

提案された品質ベクトル

```
RQI = report as a vector, not a single opaque rank:

  coverage-adjusted validated-abuse rate
  median / p90 acknowledge, triage and decision times
  mitigation effectiveness and recurrence
  false-positive and reversal rates
  median / p95 appeal-resolution time
  evidence completeness and transparency rate

Always publish N, observation window, confidence intervals,
feed coverage and malicious-registration / compromise split.
```

ガバナンスのために複合評価が必要とされる場合、評価の前に重み付けを設定し、感度分析を行い、除外された事例を用いてバックテストを実施すべきである。結果は、TLD、レジストラの規模、脅威クラス、および証拠源ごとに層別化すべきである。その結果として得られるのは、説明責任を示すシグナルであり、自動化されたドメイン判定ではない。

15

段階的アクセスを備えた公開DNS Abuse透明性データベース

透明性レジストリを導入すれば、通知の有無、その送達時期、およびそれに続く措置について生じる紛争を解消することができます。しかし、すべての証拠資料を公開してしまうと、被害者や個人データ、捜査手法、さらには現在も有効な攻撃経路が露見してしまう恐れがあります。その解決策となるのが、アクセス権限の段階的設定です。

P

公的記録

ケースID、指標、大分類、主要なタイムスタンプ、証拠の信頼度レベル、関係者の役割、結果コード、不服申立ての状態、および封印されたアーティファクトのハッシュ値。

C

契約相手先視点

再現可能な技術的証拠、連絡手段、付随する状況、および保存に関する指示。

R

権限制限付きビュー

被害者に関するデータ、資金流用の帰属分析、捜査中の資料、および編集・削除されていない証拠の保管経緯。

各更新は追記専用であり、タイムスタンプと署名が付与されます。修正によって履歴が消去されることはなく、既存の記録に上書きする形で新しい記録が追加されます。公開検索は、保存期間のルールを遵守し、被害者の一括特定を防止するとともに、不正確な個人データに対する是正措置を提供すべきです。

16

事前登録による評価を伴う6か月間のパイロット事業

有用なパイロット研究は、管理が容易な規模でありながら、因果関係の連鎖を検証するのに十分な規模であるべきです。推奨される範囲は、ボランティアのレジストラ3名、レジストリ運営者2名、ホスティング / CDNパートナー1社、独立した研究フィード2件、および適格な不服申立てパネル1つです。症例の割り当てを行う前に、研究プロトコルとアウトカムの定義を登録しておく必要があります。

第1ヶ月

プロトコルと法的マッピング

カテゴリー、権限、証拠の信頼度レベル、プライバシー影響評価、および停止条件を定義する。

第2ヶ月

既存のプロセスにツールを導入する

応答の挙動を変更することなく、ベースラインのタイムスタンプと結果を測定する。

第3ヶ月

証拠エンベロープを運用する

署名付きの証拠の来歴、重複排除、付随的影響の分類を導入する。

第4ヶ月

テスト応答ターゲット

対象となる症例を無作為に割り当てるか、ステップウェッジ法を用いて導入を進め、エラーを毎日監視する。

第5ヶ月

不服申立ての動作と失敗事例

復旧訓練の実施、レッドチームによる悪意のあるレポートの作成、およびアクセス制御の監査を行う。

6ヶ月目

独立した評価

効果量、信頼区間、欠測状況、有害事象、費用、および再現性に関する資料を公表すること。

パイロットの主要評価項目

- 検証済みのエビデンスから効果的な緩和策の実施に至るまでの時間の中央値および90パーセンタイル値。
- 通知後の帰属可能な損害の差、またはあらかじめ指定された被害者・曝露の代用指標。
- 偽陽性率、誤った措置の重大度、および回復までの時間の中央値。
- 同一の登録者、インフラクラスター、詐欺・フィッシング作戦の各レベルでの再発。
- 検証済み症例1件あたり、および有効な緩和策1件あたりの直接運営コスト。

決定規則

誤検知、プライバシー侵害、不服申立ての遅延、または付随的なサービス障害について、事前に登録された上限値を超えない範囲で、パイロット運用において実質的に迅速な実効的な緩和効果が確認された場合にのみ、規模を拡大すること。

17 結論と検証可能な提言

DNS Abuseへの対応は、純粋な技術的フィルターでも、単一の機関だけで解決できる問題でもない。2024年に発効した契約改定は実質的な緩和義務を定めた一方、証拠、時期、救済措置について相当の裁量を残している。この裁量は比例原則のために必要だが、比較可能な記録がなければ実績評価を難しくもする。

1. **証拠エンベロープを標準化する。** 報告者、レジストラ、レジストリ、インフラ事業者の間で、証拠の来歴、タイムスタンプ、結果の共通フィールドを採用する。
2. **各段階を個別に測定する。** 脅威分類と証拠レベル別に、受領確認、トリアージ、決定、緩和、不服申立てまでの時間を公開する。
3. **悪意ある登録と正規サービスの侵害を区別する。** 侵害された正規サービスではパス / アカウント単位の是正を優先し、ドメイン全体の措置は比例的である場合に限定する。
4. **対応目標を試行する。** 一律の期限を宣言するのではなく、信頼度が高く単一目的の悪意ある登録について、時間単位の目標を検証する。
5. **プライバシーを保護した形で、説明責任に関するデータを公開する。** 署名付き履歴と制限付き証拠を備えた、段階的な透明性レジストリを使用する。
6. **因果効果を評価する。** 事前登録研究が被害者への影響と攻撃の別経路への移行を測定するまでは、停止の迅速化を金銭的被害の削減と同一視しない。

建設的な結論は、当初の問題が、その主張に条件が付加されたからといって解消されるということではない。むしろ、中心的な主張を検証できるようになったということである。すなわち、検知後の被害が60 ~ 85%の範囲に及ぶという点は、明確な定量的仮説であり、 $100 ~ 150は、定義されたセンサーおよびトリアージ層に対する検証可能な工学的予算の仮定であり、また、信頼度が高く単一目的の悪意ある登録については、時間単位の対応目標を試験的に導入することができる。 作業負荷、コスト、タイムスタンプ、および結果を公表し、それらをベースラインと比較して、置換率と誤差を測定する。確認されれば、契約や方針の変更が正当化される。却下されれば、どの仮定が誤りであったかが特定される。

編集方針および研究方法に関する開示。 PhishDestroy は、独立した非営利の脅威インテリジェンス・プロジェクトです。本稿は、ポリシーおよび技術的な提案であり、法的助言、ICANNのプログラム、あるいは査読付き論文ではありません。「モデル」と表記された予算範囲は、計画上の仮定です。一次情報に基づく主張については、以下にリンクを掲載しています。訂正のご要望は、当サイトの問い合わせ窓口および責任ある開示（RD）チャネルを通じてご提出ください。

主体的な立場・説明責任は、不作為と行き過ぎの両方を抑制しなければならない

執行権限に関する個人的な境界線

私は、ドメインブロックツールへの直接アクセスを求めているわけでもなければ、それを望んでいるわけでもありません。 その権限には、独立した審査、公開された監査ログ、迅速な異議申し立て手続き、および取り消し可能性が求められます。

この業務の一部を任せることができる、有能で責任感のある企業は数多くあると私は考えています。私の経験やこれまでに公表してきた実績を踏まえると、NameSiloはそのような企業の仲間には入らないと私は考えています。

私は、米国に拠点を置く正規の企業に対し、利益相反や能力、行動規範の面で独立した精査に耐えられない特定の請負業者に、機密性の高い不正利用対策やセキュリティ業務を委託することはお勧めしません。これは国籍の問題ではなく、記録に残っている行動の問題です。ロシア出身であるという事実そのものは、米国の企業の住所が何も証明しないのと同様に、何も証明するものではありません。

私は正義と、真に意味のある説明責任を求めています 繰り返し行われた詐欺キャンペーンの一環として記録されたドメインの登録および更新から収益を得たレジストラについては、証拠が単なる過失にとどまらず、意図的な助長（直接的な運営への関与であれ、繰り返される警告にもかかわらず有害なドメインの登録とオンライン状態を維持することを役割とする、事情を知った仲介者としての行為であれ）を示唆する場合、その行為は独立した調査の対象とされ、事実が立証されれば相応の措置が講じられるべきである。 私は疑惑を既成事実として提示しているわけではないが、仲介者という立場であっても、精査から免れることはあってはならない。

基礎となる調査内容を確認する ↗

A

参考文献および出典注記

[1] **ICANN, Adopted FY27 Budget (2026)** · https://www.icann.org/en/system/files/files/adopted-icann-budget-fy2027-published-2026-en.pdf
FY27運用資金1億6,510万ドルと資金源構成の根拠。

[2] **ICANN, 2024 Global Amendment to the Registrar Accreditation Agreement** · https://www.icann.org/en/system/files/files/registrar-accreditation-agreement-global-amendment-05apr24-en.pdf
レジストラのDNS Abuse義務に関する主要な契約上の根拠。

[3] **ICANN, 2024 Global Amendment to the Base gTLD Registry Agreement** · https://itp.cdn.icann.org/en/files/registry-agreements/base-registry-agreement-global-amendment-05-04-2024-en.html
レジストリ運営者の緩和義務に関する主要な契約上の根拠。

[4] **ICANN Contractual Compliance, DNS Abuse Obligations Advisory (2024)** · https://www.icann.org/en/contracted-parties/advisories/documents/advisory-compliance-with-dns-abuse-obligations-in-the-registrar-accreditation-agreement-and-the-registry-agreement-05-02-2024-en
運用上の解釈、報告要件、適切な緩和措置の例。

[5] **ICANN, Enforcement of DNS Abuse Mitigation Requirements (2024)** · https://www.icann.org/en/system/files/files/icann-enforcement-of-dns-abuse-mitigation-requirements-08nov24-en.pdf
6か月間の実施報告書。調査件数と緩和措置件数を含む。

[6] **ICANN SSAC, SAC115: Report on an Interoperable Approach to Addressing Abuse Handling (2021)** · https://www.icann.org/en/system/files/files/sac-115-en.pdf
DNS Abuse報告の相互運用性と証拠品質に関する背景資料。

[7] **Hollenbeck, RFC 5731: EPP Domain Name Mapping (2009)** · https://www.rfc-editor.org/rfc/rfc5731.html
EPPのドメインステータス値に関する技術的な定義（サーバー側で設定されたステータスを含む）。

[8] **Laurie et al., RFC 9162: Certificate Transparency Version 2.0 (2021)** · https://www.rfc-editor.org/rfc/rfc9162.html
CTのセンサーとしての権威あるプロトコル仕様および限界。

[9] **ICANN, Centralized Zone Data Service** · https://www.icann.org/en/contracted-parties/registry-operators/services/centralized-zone-data-service
参加するgTLDゾーンファイルの適用範囲およびアクセスモデル。

[10] **FBI Internet Crime Complaint Center, 2025 IC3 Annual Report** · https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf
フィッシングやスプーフィングの件数を含む、苦情および被害届の件数。

[11] **Bijmans et al., Catching Phishers By Their Bait (USENIX Security, 2021)** · https://www.usenix.org/system/files/sec21-bijmans.pdf
データセットごとに分析したフィッシングインフラの測定結果および観測された存続期間。

[12] **Newly Registered Domains and Phishing Lifetimes, Journal of Cybersecurity (2026)** · https://doi.org/10.1093/cybsec/tyag020
新規登録されたフィッシングドメインおよびその存続期間の分布に関する最近の実証的知見。

[13] **Inferential Analysis of Maliciously Registered Domains — INFERMAL (2024)** · https://www.icann.org/en/system/files/files/inferential-analysis-maliciously-registered-domains-08nov24-en.pdf
ICANN - 資金提供を受けて実施された、悪意のある登録およびエコシステム要因に関する分析；因果関係の主張に関する関連する制約。

[14] **Chainalysis, 2026 Crypto Scam Trends** · https://www.chainalysis.com/blog/crypto-scams-2026/
2025年のオンチェーン詐欺による流入額に関するベンダーの見積もり。ドメインフィッシングの合計には含まれていない。

[15] **APWG, Phishing Activity Trends Report, Q1 2026** · https://docs.apwg.org/reports/apwg_trends_report_q1_2026.pdf
確認されたフィッシング攻撃 / URL。この数値は、登録されたドメインの総数とは一致しません。

[16] **Cybercrime Information Center / Interisle, Phishing Landscape 2025** · https://www.cybercrimeinfocenter.org/phishing-activity-numbers-may-april-2025
観測された攻撃、一意のドメイン、および悪意を持って登録されたドメインを区別します。

[17] **Verisign, Domain Name Industry Brief, Q2 2026** · https://blog.verisign.com/domain-names/q2-2026-domain-name-industry-brief-quarterly-report/
すべてのTLDにおける登録件数が4億160万件と報告されている出典。