

注目されているセキュリティ事故・事件に関する情報 ＜2018年12月版（第27号）＞（選り抜き版）

2018年12月27日
NTTデータ先端技術株式会社
セキュリティ事業部

手放したドメインの悪用

行政・企業が過去に使用したドメインを悪用する事例が現在も報告されています。企業が適切なドメインの管理を行わなかった場合、どのような被害を被る可能性があるのでしょうか。本記事ではドメインが悪用された事例を踏まえながら、ドメインの登録、運用、廃止までの各段階における対策について解説します。

手放したドメインの悪用

1. はじめに

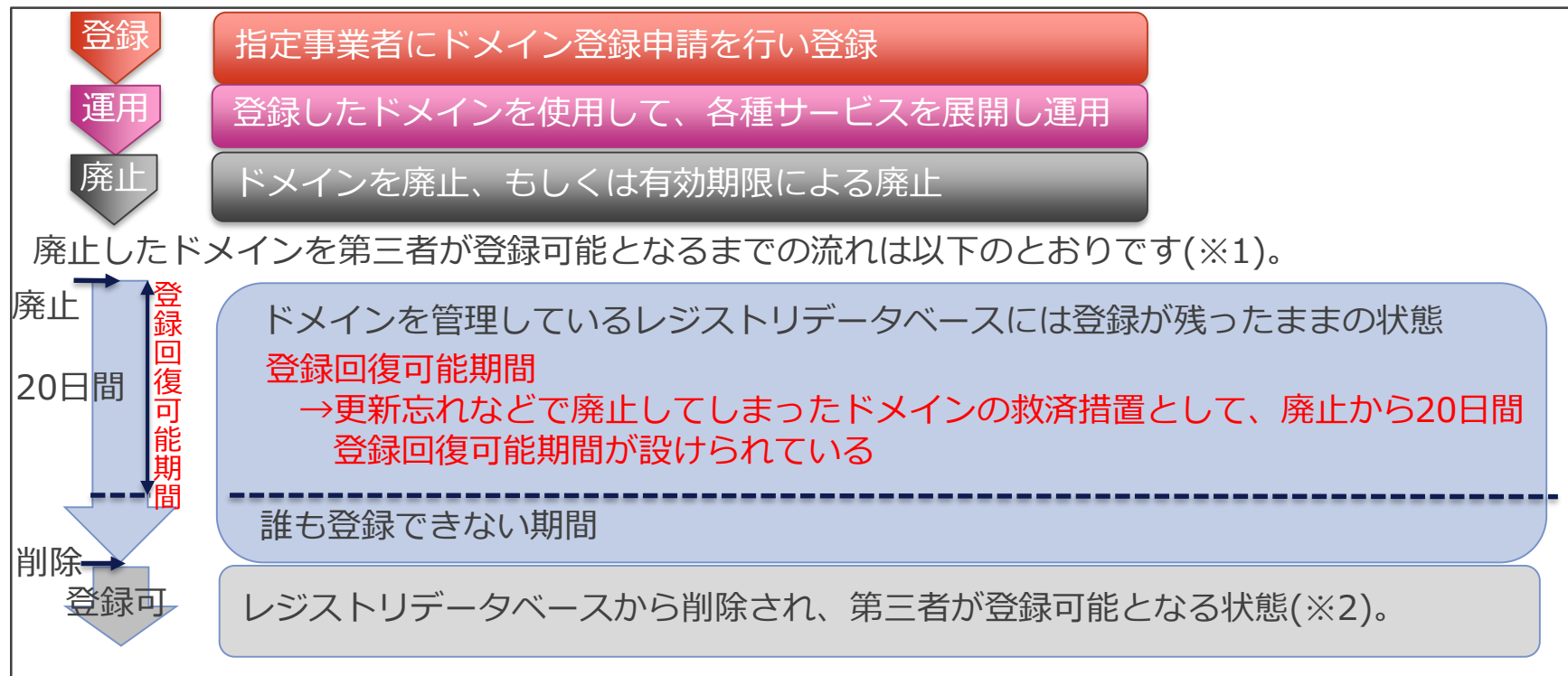
ドメインの有効期限切れを狙い、第三者が目的のドメインを登録・入手する「ドロップキャッチ」という行為が年々激しさを増しています。

実際、行政や企業が使用していたドメインが第三者の手に渡りフィッシングサイトやアダルトサイトとして再登録された事例も報告されています。また廃止したドメインを高額で販売する、中古ドメイン屋の存在も確認されています。

自社が利用したドメインが悪用されないようにするためには、ドメインの登録から廃止までのライフサイクルにおける各段階の理解と対策が必要となります。

2. ドメインのライフサイクル

一般的なドメインのライフサイクルは、以下のとおりです。



※1 本スライドではjpドメインを例にしています。「登録回復可能期間」を示す名称や日数・廃止から削除までの日数は、ドメインの種類やドメインの登録事業者であるレジストラによって異なりますので注意して下さい。

※2 第三者が登録できるドメインは種類により異なります。JPドメインの場合は以下のとおりです

- | | | |
|--------------|-------------|------------------|
| ①組織・個人問わず登録可 | 汎用JPドメイン | (〇〇.jp) |
| | 都道府県型JPドメイン | (〇〇.<都道府県名>.jp) |
| ②特定の組織ごとに登録可 | 属性型JPドメイン | (〇〇.co.jp): 企業 |
| | | (〇〇.ac.jp): 大学など |

参考 JPドメイン名の種類: <https://jprs.jp/about/jp-dom/>

3. 廃止したドメインが狙われる理由

攻撃者が廃止したドメインを狙う目的は、他のサイトからリンクが張られていたり、これまで運用されてきた実績から、ある程度のアクセスが見込めるからです。これにより、作成したWebサイトが検索エンジンで上位に表示されることになるため、アクセス数が増加して、より効率よく広告収入を得ることができるケースなどが想定されます。

また、官公庁や有名企業が使用していたドメインは信頼性が高く、訪問者を騙しやすくなるため、より狙われやすくなります。

SEO対策

- サーチエンジンでキーワード検索した際、作成したWebページが上位に表示される。(SEO : Search Engine Optimization)

アフィリエイト

- Webサイトやブログに広告を掲載して、その成果に応じて報酬を受ける。

転売目的

- アクセス数の多いサイトや信頼できるサイト(官公庁)で使用されていたドメインを高額で販売する。

フィッシングサイト目的

- フィッシングサイトを作り、個人情報やクレジットカード情報を窃取。またはマルウェア感染サイトにする。

標的型攻撃目的

- フィッシングサイトやマルウェア配布サイトを作成し、個人情報やクレジットカード情報など換金性の高い情報を入手する。

4. 企業が負う被害

廃止したドメインが悪用された場合、企業は信用を失い金銭的損害を被る可能性があります。

例えば、廃止したドメインが標的型攻撃に悪用され、取引先やグループ会社に損害が出た場合、取引先などから信用を失い、取引停止に発展する可能性があります。さらに、説明対応や損害賠償などに費用や時間、労力が割かれ、機会損失による売上低下へとつながるおそれもあります。

また、Web上の書き込みによる会社の評判の低下や風評被害などにより、新規採用者の減少や離職者の増加につながる可能性なども考えられます。

5. 悪用されたドメインの事例 (1/2)

以下にドメインが悪用された事例を示します。

項番	題名	内容	参考URL
1	地方自治体のドメインがフィッシングサイトとして悪用された	愛媛県新居浜市で使用していたドメインが第三者に登録され、オンラインカジノへ誘導するフィッシングサイトになっていた。	自治体観光サイトなりすまし被害～高い信頼性標的 https://www.yomiuri.co.jp/science/feature/CO017291/20161116-OYT8T50026.html
2	ドメインの再利用で世界盆栽大会の元URLがアダルトサイトとして悪用された	埼玉県さいたま市で行われた「第8回世界盆栽大会inさいたま」で使用されていたドメインが第三者に登録され、アダルトサイトになっていた。	ドメイン再利用で世界盆栽大会の元URLがアダルトサイトに https://cybersecurity-jp.com/news/27970
3	旧政府サイトのドメインがフィッシングサイトとして悪用された	2013年に観光庁が「タビカレプロジェクト」で使用していたドメインが悪用され、ギャンブル紹介サイトへリンクが張られたフィッシングサイトになっていた。	旧政府サイトのドメインを第三者が取得 http://www.security-next.com/093584
4	NHK関連団体のドメインがオークションに出品された	NHK関連団体の旧サイトドメインがオークションに出品された。 NHKは関連団体サイトに残っていたリンクを削除し、公式HPに注意喚起を掲載した。 最終的にドメインは13万5000円で落札された。	13万5千円で落札 = NHK関連ドメイン https://www.jiji.com/jc/article?k=2018101801125&q=soc

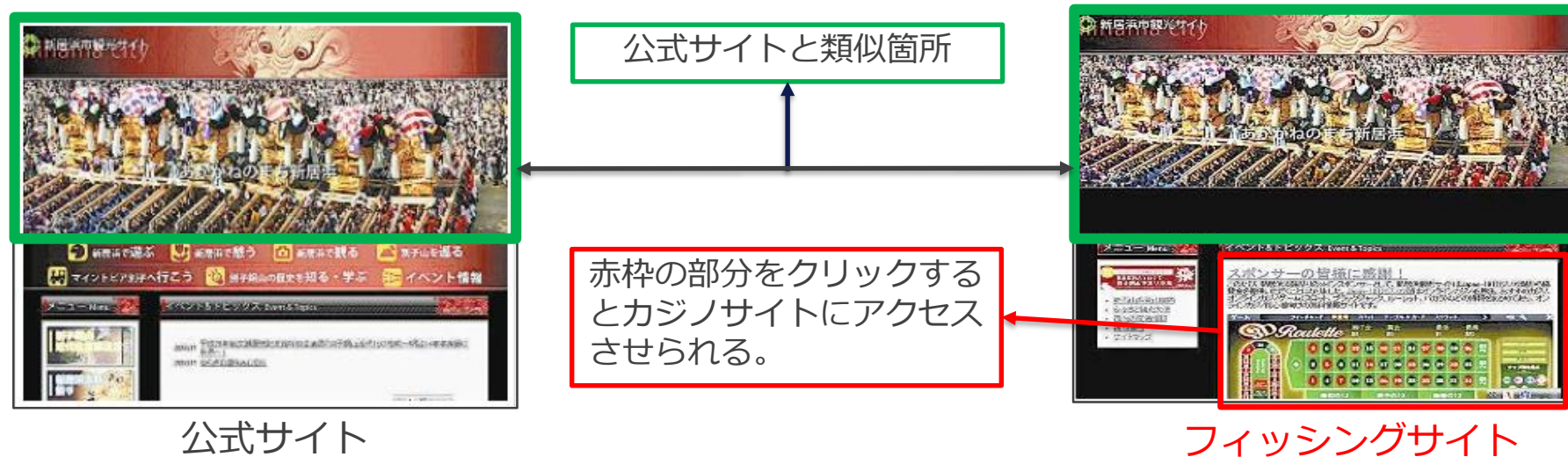
5. 悪用されたドメインの事例 (2/2)

先の表の項番 1 の事例を、詳しく紹介します。

1. 地方自治体のドメインがフィッシングサイトとして悪用

愛媛県新居浜市運輸観光課で使用していたドメインが第三者に登録され、観光課の公式サイトのフィッシングサイトになっていました。

一見して公式のサイトと見間違ふほど類似していますが、サイト内の一部でオンラインカジノ関連サイトを紹介しており、クリックするとオンラインカジノへ誘導する仕組みとなっていました。



引用：自治体観光サイトなりすまし被害～高い信頼性標的

<https://www.yomiuri.co.jp/science/feature/CO017291/20161116-OYT8T50026.html>

6. 登録時の対策 (1/2)

廃止したドメインを悪用されるケース以外においても、ドメインを悪用されないようにするためには、ドメインのライフサイクルに沿った対策が必要となります。

以下に示す対策の実施を検討して下さい。

【登録時の対策】

1 ガイドラインの制定

運用に関するガイドラインを制定し、ドメインの登録から廃止まで計画的に進めます。特に登録するドメインが多いと管理が煩雑となり、リスクも高まるため、登録前にドメイン取得の必要性について十分に検討する必要があります。

2 ドメインの維持費用の計算

運用予定期間だけではなく、ドメインを用いた運用終了後も一定期間更新して、維持することが重要です。

また登録時の段階で慎重に検討し、更新費用を予算に組み込みます。

3 類似ドメインの登録

フィッシングサイト、標的型攻撃の未然防止のため、登録予定ドメインに類似するドメインも登録します。

例 example.co.jpを登録予定とした場合

exam n ple.co.jp	(タイプミス	:「m」が「n」)
exam 1 e.co.jp	(似ている文字を使う	:「l」が数字の「1」)
example. com	(トップドメイン	:「co.jp」が「com」)

6. 登録時の対策 (2/2)

4 登録予定ドメインの文字列が他社の商標ではないか確認

商標権に抵触する場合、他社からの請求により訴訟に発展するおそれがあります。
登録前に商標権に抵触しないか調査します。

5 ドメインの登録情報に関する連絡先確認と非公開設定

登録情報はインターネット上のWHOISで検索可能となるため以下の点に留意します。

(1) 登録担当者・連絡先のメールアドレス

登録したメールアドレスには、更新のお知らせなど重要な通知が来るので、数人でチェックできるように個人のものではなく、担当部署のメールアドレスを使用するなど、複数の関係者が閲覧できるものにします。

(2) 連絡先メールアドレスの非公開設定

レジストラ(ドメインの登録事業者)によってはメールアドレスの表示をブロックしたり、登録情報を代理公開したりするサービスがあります。代理公開することにより、連絡窓口の氏名やメールアドレス、連絡先などを登録事業者の情報に代えて掲載することができます。

- ・メリット : 標的型攻撃のリスク低減、スパム対策となる
- ・デメリット : 善意者からの技術的トラブルなどの連絡が来なくなる

7. 運用時の対策

1 ドメインの更新

ドメインの更新を忘れ、さらに登録回復可能期間に手続きをしなかった場合、ドメインは第三者が登録可能状態となります。確実な更新のため自動更新申請をします。

2 登録・連絡先情報の更新

担当者が異動した場合は、速やかに登録情報を更新します。

3 類似ドメインによる悪用がないかWeb & WHOISチェック

登録したドメインに類似するフィッシングサイトがないか監視します。
発見時の対応例を以下に示します。

項目	内容
安全なサイトであるかの確認	サイトがどのような目的で使用されているかを確認し、自社を狙ったフィッシングサイトの可能性がある可能性がある場合は、ID・パスワードなどの認証情報の入力を求めているか、マルウェアを配信をしていないかを調査します。
アクセス遮断	悪意のあるサイトの場合は、自社の社員が意図せずアクセスして認証情報などを入力しないようにするために、ProxyサーバやFWなどでブラックリストに登録し、自社から通信できないように遮断します。また、ISP、JPCERT/CCにサイトの停止依頼をします。
顧客・取引先への通知	自社のWebに注意喚起のお知らせ文などの掲載を行います。

4 ドメインが悪用され、自社の商標が侵害された場合

自社の商標が侵害され、悪意をもって使用されている場合は、ドメイン奪還の必要性を検討します。奪還することとした場合、ドメイン紛争処理の申し立てを行い、ドメインの取消・移転を行います。

参考：偽JPCERTドメイン名を取り戻すための60日間
<https://blogs.jpCERT.or.jp/ja/2017/05/udrp.html>

8. 廃止時の対策

1 ドメインを更新維持する場合

廃止したドメインの悪用を防ぐため、当面の間もしくは永久的に更新をします。当面の間の目安としては、サーチエンジンで検索しても検索結果に表示されなくなるまで保持することをおすすめします。

永久にドメインを保持することでリスクを完全に排除できますが、ドメインの維持管理には更新費用も管理稼働もかかります。「登録時の対策」で挙げたとおり、ドメイン取得の必要性を検討し、必要性の低いドメインは取得しないなど、ガイドラインに沿って計画的に運用することでトラブルを防ぐことができます。

2 ドメインを廃止する場合

ドメインを廃止する場合はリスクを再検討します。その上で廃止が決定し、ドメインを手放す場合は、第三者が登録することを前提として、以下の対策を取ります。

(1) 廃止したドメインの定期的な監視

定期的にドメインの利用状況をWHOISで確認し、悪意のあるサイトとして使用されていないかを監視します。

また、有償ではありますが代行して監視してくれるサービスもあります。

(2) リンクの確認

自社が管理するWebサイトに、廃止したドメインへのリンクがないことを確認します。

3 更新忘れにより、やむを得なく廃止してしまった場合

ドメインの種類やレジストラによっては、登録回復可能期間があるため、再度登録申請を試み更新をします。

9. まとめ

本記事では、企業が廃止したドメインが再利用されて悪用された事例を踏まえながら、企業が被る可能性のある被害と、取り得る対策について解説しました。

ドメインの管理は、ドメイン廃止時のみ対応しがちですが、ドメイン登録時において、ライフサイクルを踏まえて対策を検討することにより、その後のリスクやトラブルを低減することができます。

貴社で制定されているドメイン運用のガイドラインに、本記事で示した注意すべき点を盛り込み運用することで、自社を守るだけでなく、取引先やお客様など第三者をも守ることにつながります。

10. 参考URL

- JPドメイン名の種類
<https://jprs.jp/about/jp-dom/>
- 偽JPCERTドメイン名を取り戻すための60日間～ドメイン名紛争処理をしてみた～
<https://blogs.jpCERT.or.jp/ja/2017/05/udrp.html>
- ドメイン名を放棄するのは危険 その脅威と対策とは
<http://ascii.jp/elem/000/001/768/1768974/>
- ドメイン名登録の際の注意
<https://jprs.jp/registration/cyber-squatting/>
- 削除済ドメイン名のための「請戻猶予期間」
<https://www.nic.ad.jp/ja/dom/gtld-policy/rgp.html#id0002>
- 自治体観光サイトなりすまし被害～高い信頼性標的
<https://www.yomiuri.co.jp/science/feature/CO017291/20161116-OYT8T50026.html>
- ドメイン再利用で世界盆栽大会の元URLがアダルトサイトに。
<https://cybersecurity-jp.com/news/27970>
- 旧政府サイトのドメインを第三者が取得。
<http://www.security-next.com/093584>
- 1 3 万 5 千円で落札 = N H K 関連ドメイン
<https://www.jiji.com/jc/article?k=2018101801125&g=soc>

