群馬県警察 Gunma.Pref.Police
部外用
サイバーセキュリティ対策通信 令和２年度 第５号

廃止ドメインの悪用が相次いで発生！！

～ドメインの使い捨て、設定変更漏れにご注意～

公的機関が過去に利用していたドメインが第三者の手に渡り、全く関係のない組織で商業利用を含め、悪用されてしまう事案が相次いで発覚しています。

もし、組織で利用していたドメインが犯罪に利用されてしまうと、廃止したドメインであったとしても、その組織の信用が失墜してしまいます。

廃止ドメインの悪用手口①
ドロップキャッチ

登録期限が切れたドメイン名を、再登録が可能になるタイミングを狙って第三者が取得することを言います。

公的機関や有名企業で利用されていたドメインは、SEO（検索エンジンの最適化）の面で価値が高く、ドロップキャッチで狙われやすい傾向があります。

【ドロップキャッチの例　イメージ図】

①ドメイン「example.jp」の登録期限切れ

③ドメイン名「example.jp」が登録可能状態になったことを確認して同名で登録申請（早い者勝ち）
→ **ドロップキャッチ**

④同じドメイン名で別サイトを作成
→ **アダルトサイトや商業サイトとなる例も…**

≪対策・注意≫

安易にドメイン名を使い捨てしないようにしてください！

一度、第三者の手に渡ってしまったドメインは、簡単に取り戻せません。

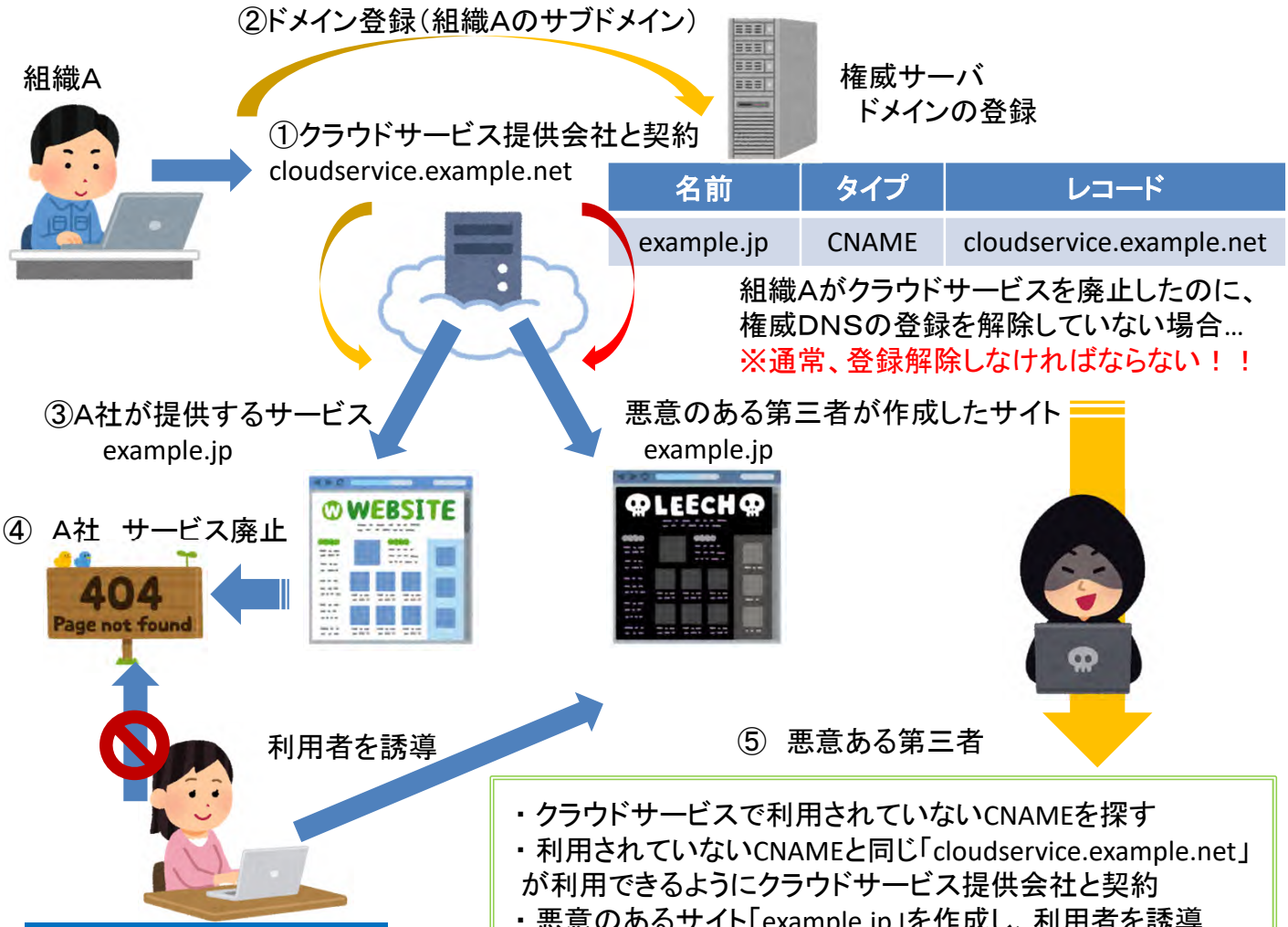
ドメインを新規に登録する前にサブドメインを活用するなどして、新規サービスの運用を検討しましょう。

廃止ドメインの悪用手口②
ドメインテイクオーバー

外部サービスの利用開始時に設定したドメイン（サブドメイン）のDNS設定（CNAME）がサービス終了後も残ったままとなっていることを利用し、悪意のある第三者が、そのドメインを乗っ取る手法です。

ドメインを乗っ取られた場合、利用者がアクセスしようとすると、悪意のある第三者が作成したサイトへ誘導されてしまいます。

【ドメインテイクオーバーの例　イメージ図】



・クラウドサービスで利用されていないCNAMEを探す
・利用されていないCNAMEと同じ「cloudservice.example.net」が利用できるようにクラウドサービス提供会社と契約
・悪意のあるサイト「example.jp」を作成し、利用者を誘導

≪対策・注意≫

外部サービスを廃止した場合、
『権威DNSの登録』は確実に解除してください！

サービスの廃止では、組織内のシステム設定や構成変更には目が届きますが、外部へ設定（DNSの登録等）を忘れがちになりますのでご注意ください。

廃止ドメインの悪用は、利用者がブックマーク等で再度訪問した場合、悪意のある第三者が作成したサイトに誘導されるため、サービスが乗っ取られていると感じる場合や不正プログラムをダウンロードさせられる可能性もありますので、ドメインを悪用されないように管理しましょう。

＜群馬県警察本部警務課サイバーセキュリティ対策係　℡027-243-0110 ＞