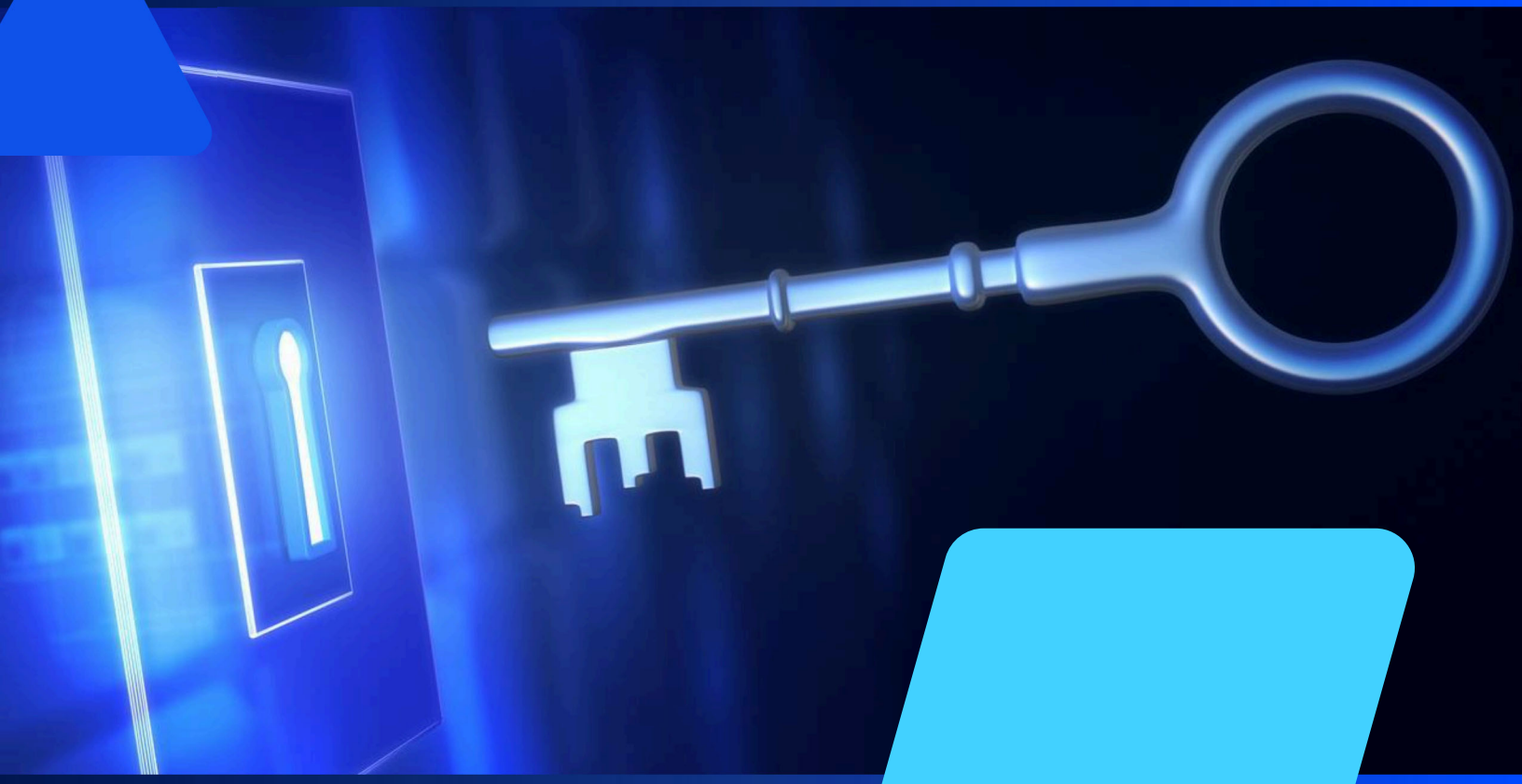
レジストリロック：

見落とされがち。でも、ドメインを守るために必要不可欠



Markmonitor™

著者の紹介：

商業戦略担当責任者、Bonnie Wittenburg

業界で30年近い経験を持つBonnieは、世界有数の大手企業に対し、強固なドメイン名管理戦略の構築を支援してきました。国際的な企業で見られる複雑性への対応、コスト削減のためのポートフォリオの最適化、そしてプロセスの簡素化を専門としています。

Bonnieの専門性は、多様で複数の関係者を抱える企業の複雑なニーズに対応し、セキュリティの確保と予算上の制約の両立を図るための、オーダーメイドの戦略を策定することにあります。Markmonitorは、商業戦略担当責任者としてBonnieをリーダーシップチームの一員に迎えられることを嬉しく思います。

軽視してはならない重要な防御策

私は、ドメイン管理者がポートフォリオのセキュリティ体制を強化するうえで役立つヒントや知見を、よく尋ねられます。推奨される対策のひとつは、**レジストリロックの導入です。これは十分に活用されていないことが多い一方で、企業のデジタルプレゼンスを守るうえで極めて重要なセキュリティ対策となります。**

レジストリロックがあれば、レジストラはレジストリと直接連携して、適切な認証と承認が完了しない限り、ネームサーバーの更新、連絡先の詳細の編集、ドメインの転送などの不正な変更をブロックします。これは、業務上重要なドメインをミス、攻撃、不正なアクティビティから保護するのに役立ちます。

レジストリロックは、ドメインのハイジャック攻撃、DNSの改ざん、不正な移管に対する極めて有効な防御策です。驚くべきことに、数多くのポートフォリオにおける導入状況は、依然として低水準にとどまっています。実際、トップ500企業のうち半数未満しか、最重要ドメインにレジストリロックを設定していません。[1]

このことから、レジストリロックが強力な保護手段として広く認められているにもかかわらず、なぜ多くの企業が導入を検討しないのか、その理由を調査することにしました。

ここからはその調査結果を紹介します。

導入における障壁

認識の不足
多くの組織は、ドメインの脆弱性に気づいておらず、レジストリロックという仕組みが存在することさえも認識していません。標準的なレジストラロックや2要素認証で十分であると考えられています。

1. Brand Finance, Global 500 2024

軽視してはならない重要な防御策

セキュリティ部門やIT部門は、エンドポイントの保護、ファイアウォール、クラウドセキュリティに重点を置く傾向があり、その結果、ドメインセキュリティは見落とされがちです。標準的なセキュリティ監査の対象として扱われないことが多く、実際にインシデントが発生して初めて痛みを伴う形で、ドメインセキュリティを優先すべきだと学ぶケースも少なくありません。

例：不注意にも従業員が、レジストラからのものだと思い込み、フィッシングメールに引っかかってしまうケースがあります。ログインし、そして知らないうちに認証情報を渡してしまいます。攻撃者はアクセス権を得ると、ドメイン設定を変更することや、ドメインを外部へ移管すること、さらにはトラフィックを不正サイトへリダイレクトすることさえ可能になります。レジストリロックを導入していれば、こうした不正な変更はレジストリレベルで防げていたはずです。信頼性の高いレジストラを利用し、レジストリロックを設定しておくことは、深刻な被害を未然に防ぐための有効な手段となります。

業界標準の欠如

すべてのTLDやレジストラがレジストリロックをサポートしているわけではありません。仮に対応していても、その導入方法は異なる場合があります。

一貫性のなさが、統一的なドメイン保護ポリシーの策定を難しくしており、利用可能な保護策を理解し実装するうえで、企業向けドメインレジストラが、重要な資産であることを浮き彫りにしています。

例：.COMドメインの場合、自動処理と手動処理を組み合わせたプロセスの中で、レジストリ（例：Verisign）が関与し、変更には多要素認証が求められます。ドメイン所有者とレジストラ、さらにVerisignの3者が連携し、変更が行われます。.UKドメインの場合、レジストリ（例：Nominet）は「レジストリロックサービス」と呼ばれる方式を採用しています。これは.COMよりも手動処理に依存したプロセスであり、更新にはセキュアなパスワードと手動による確認が必要となります。Markmonitorのような信頼性の高い企業向けレジストラは、組織が多様なプロセスを理解できるよう支援し、導入に至るまでアドバイスとサポートを提供します。

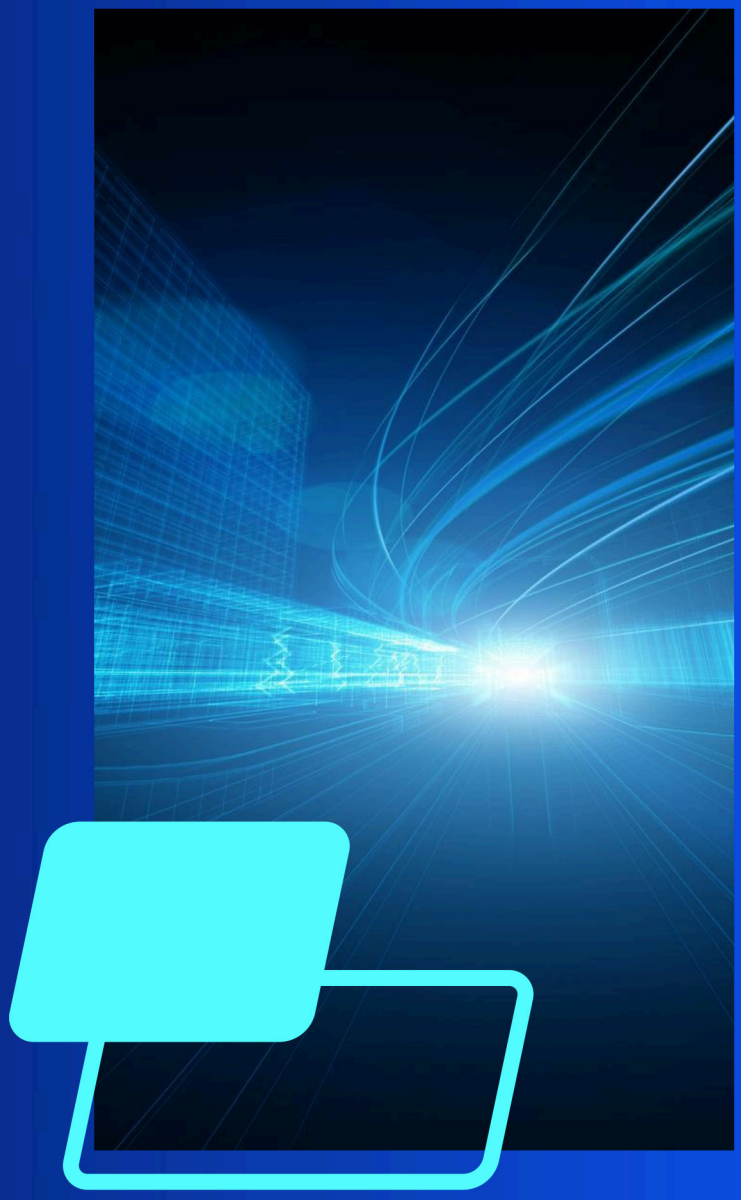
...一貫性のなさが、統一的なドメイン保護ポリシーの策定を難しくしており、企業向けドメインレジストラが重要な資産であることを浮き彫りにしています。

軽視してはならない重要な防御策

複雑さと不便さ
レジストリロックは、多くの場合、特定のドメインに変更を加える際に、ある程度手動処理のプロセスを必要とします。これらのプロセスには通常、レジストラとレジストリの双方が関与し、場合によっては、電話でのやり取り、署名付きの申請、あるいは複数の当事者による承認が必要となります。

セキュリティ面では優れていますが、俊敏性を求めるITチームにとっては不便さを感じるものです。DNS変更や連絡先情報の修正など、頻繁な更新を要するドメインでは、特に、そのドメインが事業上、不可欠であると見なされていない場合は、ロック解除と再ロックの手間が負担に感じられることがあります。しかし、レジストリロックには、レジストラやレジストリによる追加の人員やサポートを必要とするという事実こそが、レジストリロックが存在し、かつ有効である理由なのです。

例： フィッシングメールに引っかかり、不注意にも攻撃者にログイン認証情報を渡してしまった従業員の例を思い出してください。レジストリロックが設定されているドメインに対して、攻撃者はいかなる変更も行うことはできません。



レジストリロックの プロセスによる抑制と均衡が、攻撃者によるフィッシングの悪用を阻止します。

軽視してはならない重要な防御策

費用とリソースの制約
レジストリロックには通常費用がかかるため、小規模な企業ではそのための予算を確保していない場合があります。また、特に経営層がリスクを十分に理解していない場合、追加費用は不合理に思えることもあります。しかし、ダウンタイムが一度発生するだけで、収益の損失や深刻なダメージにつながり、企業に多大な損害をもたらす可能性があります。事前に対処することで、のちに発生する損失を回避することができます。

例：不要な費用だと考え、企業は自社の事業にとって重要なドメインに対してレジストリロックを購入していません。そして災難が襲います。ドメインのハイジャック攻撃によって主要サイトが停止し、収益と企業の信頼性が大きく失われます。ロックを導入していなかったことによる代償が明らかになるにつれ、当初の節約は意味を失います。

重要でありながらも見落とされがちな重要ツール

いくつかの障壁はあるものの、レジストリロックは価値の高いドメインに欠かせません。銀行、政府のポータルサイト、医療機関、あるいはドメインが信頼性やアップタイムと直結しているあらゆる企業が、その対象となります。

> **ダウンタイムが一度発生するだけで、収益の損失や深刻なダメージにつながり、企業に多大な損害をもたらす可能性があります。**

一度でもハイジャック攻撃を受ければ、フィッシングやデータの流出につながり、企業の信頼性は大きく揺らぎます。

トレンドの変化
。ポジティブな傾向導入は拡大しており、特に大企業やセキュリティを重視する企業の間で顕著です。 **DNSハイジャック攻撃や、レジストラレベルでの攻撃が増加するにつれ、このシンプルながら効果的なツールへの注目も高まっています。レジストリロックは、単なるベストプラクティスではなく、もはや不可欠なものであると多くの組織が認識し始めています。**

ドメインポートフォリオを管理している場合、特に上場企業や標的にされやすいブランドに対しては、Markmonitorがレジストリロックを効果的に導入する方法をご提案します。

Markmonitorは、世界のトップブランドの収益と評判を保護するための、戦略的なドメイン管理ソリューションを提供しています。

1999年創業以来、私たちは世界で最もアクセス数の多いさまざまなウェブサイトを含む、世界中の企業のドメインポートフォリオのニーズに応えてきました。ICANN認定ドメインレジストラとして、Markmonitorは業界で築いた強い関係性、革新的なテクノロジー、幅広い専門知識を活用し、ドメインポートフォリオの価値を最大化するデータ主導のきめ細かいコンサルテーションにより、企業のドメインポートフォリオを管理し保護しています。

さらに詳しい情報やサポートが必要な場合は、アカウントマネージャーにお問い合わせいただくか、 customer.service@markmonitor.com までメールでお問い合わせください。

Markmonitor