セキュリティの総合評価を左右するエンタープライズクラスのドメインレジストラ導入

SecurityScorecard.com
info@securityscorecard.com

214 West 29th St.,5th Floor
New York, NY10001
1.800.682.1707

SecurityScorecard CSC

はじめに

ランサムウェア攻撃、ビジネスメール詐欺(BEC)など、ほとんどのサイバー攻撃はフィッシングから始まります。ランサムウェア攻撃の初期段階では、フィッシングが出発点となるのです。ランサムウェアによる被害は、今や年間数十億ドル[1]に上りますが、ランサムウェア対策のほとんどは、フィッシングリスクに対して適切に対応できていません。

定評のある調査によれば、フィッシング攻撃は通常、悪意に基づき登録された紛らわしいドメイン名や、乗っ取られた正規ドメイン名、あるいはなりすましメールなどを通じて行われます。エンタープライズクラスのドメインレジストラを利用することで、こういったリスクを回避することができます。

どのドメインレジストラを使っているかは、企業や機関の総合的なセキュリティ体制を示す指標となります。

SecurityScorecardの調査によれば、ドメインレジストラの選択は、組織のサイバーセキュリティの評価と深く関連していることが分かっています。ドメイン管理にエンタープライズクラスのレジストラ(ECR)を採用した組織は、一般消費者グレードのドメインレジストラ(CGR)を選択した組織に比べ、合計スコアが平均して0.5から1ランク高くなっています。

エンタープライズクラスの
レジストラの特徴

ドメインレジストラには、一般消費者グレードのレジストラとエンタープライズクラスのレジストラの2種類あります。一般消費者グレードのレジストラは、ドメインサービスやウェブサイト、個人や中小企業向けの電子メールを中心としたサービスです。CGRが悪いという訳ではありませんが、ドメインセキュリティ機能や制御、知的財産保護を重視したサービスを提供している業者はほとんどありません。

一方エンタープライズクラスのレジストラは、高度なサービスやツールによるドメインセキュリティを重視し、サイバーセキュリティと知的財産保護を使命とし、重点的に取り組んでいます。さらに、小売ウェブサイトやクリック課金、ドメインスピニング、知的財産や商標の侵害を助長するドメインオークションサービスを通じてドメインサービスを提供することはありません。

エンタープライズクラスのレジストラを見分けるための、主な特徴は次の通りです：

- **全社的規模と専門性**
  企業専用ドメイン、DNSおよび証明書管理サービスを提供。
- **高度なサービス**
  ドメインレジストリロック、DMARC、DNSSEC、CAAレコード、DNSホストの冗長性などが可能。
- **世界中で24 時間 365 日の現地サポート体制を提供し、**
  世界各国でドメイン登録サービスが可能。
- **Know Your Customer (KYC)**
  手法を用いた顧客情報の収集と検証。
- **ドメイン・ブランド・詐欺の監視**
  保護・テイクダウンサービスを提供。

フォーブス誌グローバル2000企業のドメインセキュリティ評価

2021年CSCドメインセキュリティ報告書により、グローバル2000企業では事業や運用の最新化が進んでいる一方で、ウェブドメインは依然として危機的なほど保護が行われていない状況であることが分かりました。2021年は企業がランサムウェア攻撃、ビジネスメール詐欺、フィッシング攻撃、サプライチェーン攻撃、オンラインブランドや商標の悪用などの被害に会うケースが増加しましたサイバーリスクの高まりにもかかわらず、フォーブス誌グローバル2000企業による対策の水準は変わっていない状況です。

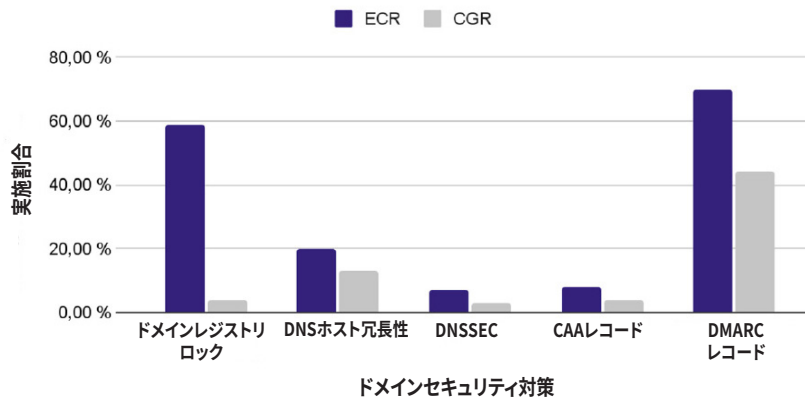
報告書の主な調査結果は、フォーブス誌グローバル2000企業が直面しているドメインセキュリティのリスクを浮き彫りにしています。

- **紛らわしい文字列のドメイン** (あいまい一致) – フィッシング詐欺やブランドの乱用の手口としてよく使われるこの手口の70%は、サードパーティが所有し、一般消費者グレードのレジストラで登録されている。
- **このようなドメイン登録のうち60%**が過去2年以内に登録されたものであり、この攻撃手法が急激に増加していることを示している。
- **企業の81%**はドメインレジストリロック手順など、基本的なドメインセキュリティ対策を導入していないため、ドメイン名やドメインネームシステム(DNS)ハイジャックのリスクが高くなっている。
- **企業の57%は一般消費者グレードのドメインレジストラに依存しているため**、ドメインやDNSのハイジャック、分散型サービス拒否(DDoS)、中間者攻撃(MitM)、DNSキャッシュポイズニングに対する保護が不十分である。
- **DMARCを導入しているのはわずか50%。**

またこの調査では、ECRグループとCGRグループのドメインセキュリティ対策の実施状況を比較することで、結果が立証されています。

フォーブス誌2000社によるドメインセキュリティ対策の実施状況

ECRグループとCGRグループの比較



エンタープライズクラスのドメインレジストラを使用することで、SecurityScorecardの総合評価を0.5〜1ランク上げることができます。

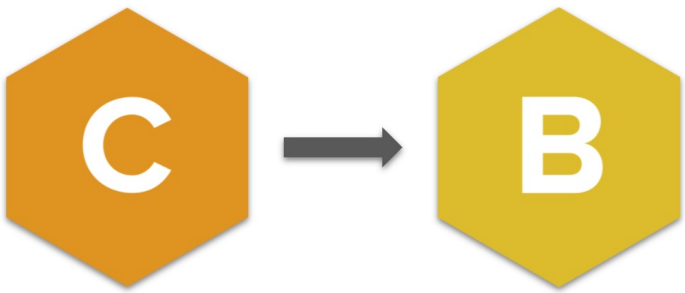
セキュリティ評価により、ドメインセキュリティを優先する必要性が明らかに

SecurityScorecardは、同社のプラットフォームにおいて最もフォローされている50,000社のセキュリティ評価を分析。その結果、信頼できるエンタープライズクラスのドメインレジストラを使用し、ドメインとDNSセキュリティを優先する必要性があることがまた明確になりました。ドメイン管理にエンタープライズクラスのレジストラを選択した企業の格付けは、一般消費者グレードのレジストラを使用している企業よりも平均で少なくとも0.5ランク高くなっています。CSCの分析では、これは総合格付けで「B」と「C」の違いになります。

SecurityScorecardの調査により、ドメイン名レジストラの選択は、非常に重要ながら見落とされがちであるが、組織の総合的なセキュリティ体制の強化に貢献することが確認されました。

エンタープライズクラスのドメインレジストラが組織のセキュリティ総合評価に与える影響を数値で表す

SecurityScorecardが分析した50,000社の組織のうち、消費者グレードのレジストラを使用している組織は、SecurityScorecardの平均評価が76.92ポイントでした。一方でエンタープライズクラスのドメインレジストラを使用している組織では、SecurityScorecardの平均評価が81.73ポイントと、平均で5ポイントの差がありました。これは、ECRグループとCGRグループで、格付けが「C」から「B」にアップするほどの差になります。



DNSの健全性は重要な評価基準であるにもかかわらず、リスク要因としてランキングが最も低いことが判明

SecurityScorecardプラットフォームは、OpenResolver構成をはじめ、DNSSEC、SPF、DKIM、DMARCなど推奨構成が設定されているかなど、複数のDNS設定を評価しています。

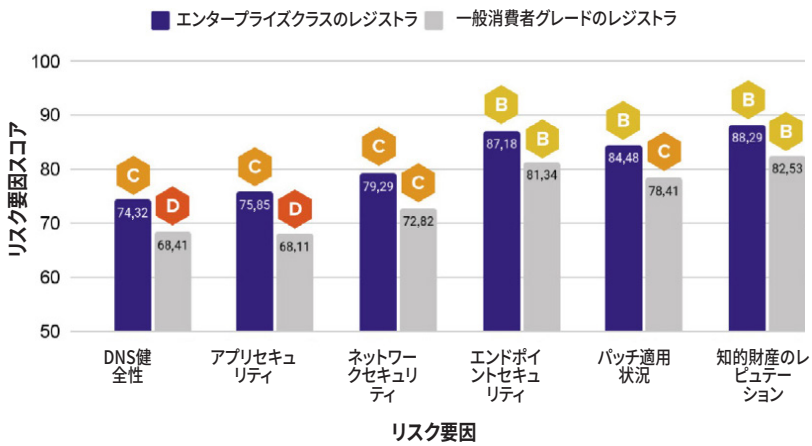
SecurityScorecardの評価アルゴリズムでは、重要な評価基準とされているにもかかわらず、分析した企業のDNS健全性の平均スコアは71.36 (格付け: C) でした。
そのためDNS健全性は、分析されたリスク要因スコアの中で最も低い評価という結果になったのです。SecurityScorecardのDNS健全性の平均的なリスク要因評価は、ECRグループが74.32であったのに対し、CGRグループは68.41となり、平均で6ポイント近い差が出ています。 格付けでは両者間でCとDの1段階分かれる結果となります。

DNS健全性は他の主なリスク要因にも影響

また当社の調査により、アプリ、ネットワーク、エンドポイントの各セキュリティ、パッチ適用状況、知的財産のレピュテーションなど、他のリスク要因評価でも、ECRグループとCGRグループでは5ポイント以上の差があり、その結果複数の要因評価で1ランクの差がついていることも分かりました。

平均リスク要因スコア

ECRとCGRの比較



この分析から、積極的にドメインセキュリティ対策を採用することで、DNS健全性を強化するのみならず、他の要因評価も向上し、結果として、セキュリティの総合評価が高くなっていることが分かります。

CSCとSecurityScorecardは、サイバーリスク対策の基盤を築くアライアンス

CSCは、セキュリティ格付けで世界有数のSecurityScorecardと戦略的提携を結び、ドメインセキュリティに関するインサイトをお客様に提供できることになりました。攻撃からドメインとDNSを保護するために極めて合理的かつ積極的な対策を講じることにより、組織とサイバー保険会社は、企業ブランドのフィッシング乱用や違反などが発生する前に、潜在的なサイバーリスクをピンポイントで見つけ出すことができます。

ドメインのセキュリティには、高度なセキュリティ対策と運用手順による多層防御手法が必要ですが、SolarWindsのような攻撃がサプライチェーンにダメージを与えていることからも分かるように、レジストラの種類を慎重に選ぶことも非常に重要です。従来のDNSセキュリティの見方は、DNSの回復力、解決、および関連するDDoS保護に重点を置いていました。今日見過ごされているDNSヘルスの重要な要素は、企業やその消費者に対して悪意ある攻撃を行うため、ドメインやDNSがどう使われているかという点です。

ドメインセキュリティにおける3つの柱

CSCが注目する3つのドメインセキュリティ

1. ドメインレジストラやDNSホストプロバイダーで、正規ドメインとそれに紐づくDNSが侵害されていないことを確認する(DNSハイジャック、ドメインハイジャック、サブドメインハイジャック)。
2. 悪意あるサードパーティードメインを監視し、停止させる。
3. なりすましメール対策として、Eメール認証が行われていることを確認する。

CSCドメインセキュリティによるベストプラクティス

あらゆる産業のあらゆる企業、特に新型コロナ感染の影響にさらされている企業は、複数の防御レイヤーで構成される多層防御手法をドメインセキュリティに採用する必要があります。そのためにはまず、エンタープライズクラスのドメインレジストラを利用することが重要です。

CSCは次の4つの重要な戦略を推奨しています:

1. ドメイン管理に多層防御手法を導入。
2. ドメインレジストラの業務手法が、詐欺やブランドの乱用の原因となっていないことを確認。
3. ブランドの乱用、侵害、フィッシング、詐欺行為がないか、ドメインやDNS空間をはじめ、アプリやソーシャルメディア、Eメールなど、主要なデジタルチャネルを継続的に監視。
4. テイクダウンおよび高度なインターネットブロッキング技術など、グローバルな保護。

結論

ランサムウェアが急激に拡散し続け、リモートワーク推進により新たなセキュリティ上の問題も発生していることから、信頼できるドメイン名レジストラを選ぶことが、サイバーセキュリティのリスク低減やオンラインブランド保護の責任者にとって重要な決断となってきています。セキュリティ、データ管理、グローバルサポートを優先するエンタープライズクラスのレジストラを選択することが、組織のブランドや顧客の安全を守るためには不可欠です。

SecurityScorecardとCSCは、ドメインセキュリティ対策の欠如により起こり得る様々なリスクを周知し、低減できるよう力を合わせて取り組んでいます。その対策は何よりもまずドメイン名レジストラの正しい選択から始まるのです。

最後に

自社とベンダー最大5社までモニタリングが可能「SecurityScorecard Enterprise License」はこちらから無料で登録できます。

CSCドメインセキュリティ
監査の無料登録はこちらから。

[1] https://www.forbes.com/sites/forbestechcouncil/2021/04/30/why-ransomware-costs-businesses-much-more-than-money/?sh=75f066bf71c6

関連資料

ベストプラクティスの全リスト:

2021年版CSCドメインセキュリティ報告書

CSCブログ

最新のサイバーリスク管理チームを構築する5つのステップ

パーフェクトな評価結果を目指して:サイバーセキュリティ格付けで取締役会からAランクを獲得する

SecurityScorecardブログ

CSC概要

CSCは企業向けドメイン名、DNS、デジタル証明書管理、デジタルブランド保護・ネット詐欺・フィッシング詐欺詐欺からの保護サービスのプロバイダーとして、フォーブス誌「グローバル2000」や「Best Global Brands®100社」に名を連ねる多くの企業に選ばれています。当社は、独自のセキュリティソリューションを用いて、サイバー脅威からオンライン資産を保護し、壊滅的な収益の損失やブランドイメージの低下、多額の罰金などを回避できるよう企業をサポートしています。
また、オンラインブランド監視と保護を組み合わせ、デジタル資産保護のための包括的アプローチを提供しています。ドメイン管理、セキュリティ、ブランド保護、詐欺からの保護サービスなどのサービスについての詳細は、cscdbs.comをご覧ください。

SecurityScorecard概要

SecurityScorecardは、継続的かつ非侵入型の監視を通じて、企業が自社およびサードパーティのセキュリティ体制を運用管理できるよう支援しています。SecurityScorecardは、ハッカーと同様の手法を用い、外部の視点から脆弱性を特定することを重視したアプローチに焦点を当てています。
SecurityScorecard独自のSaaSプラットフォームは、アプリセキュリティ、マルウェア、パッチ適用状況、ネットワークセキュリティ、ハッカー傍受、ソーシャルエンジニアリング、情報漏えいなど、様々なリスクを含む重要なデータポイントを、どこよりも幅広くかつ深く掘り下げて提供しています。

お客様の会社の現在の評価をメールでお知らせいたします。詳しくは instant.securityscorecard.comをご覧ください。

www.securityscorecard.com
1 (800) 682-1707
info@securityscorecard.com
@security_score

SecurityScorecard本社
214 West 29th St., 5th Floor
New York, NY 10001