サイバーセキュリティ体制とドメイン名管理の交差点

CSC インサイトペーパー

Contents

サイバーリスクを AI のスピードで管理

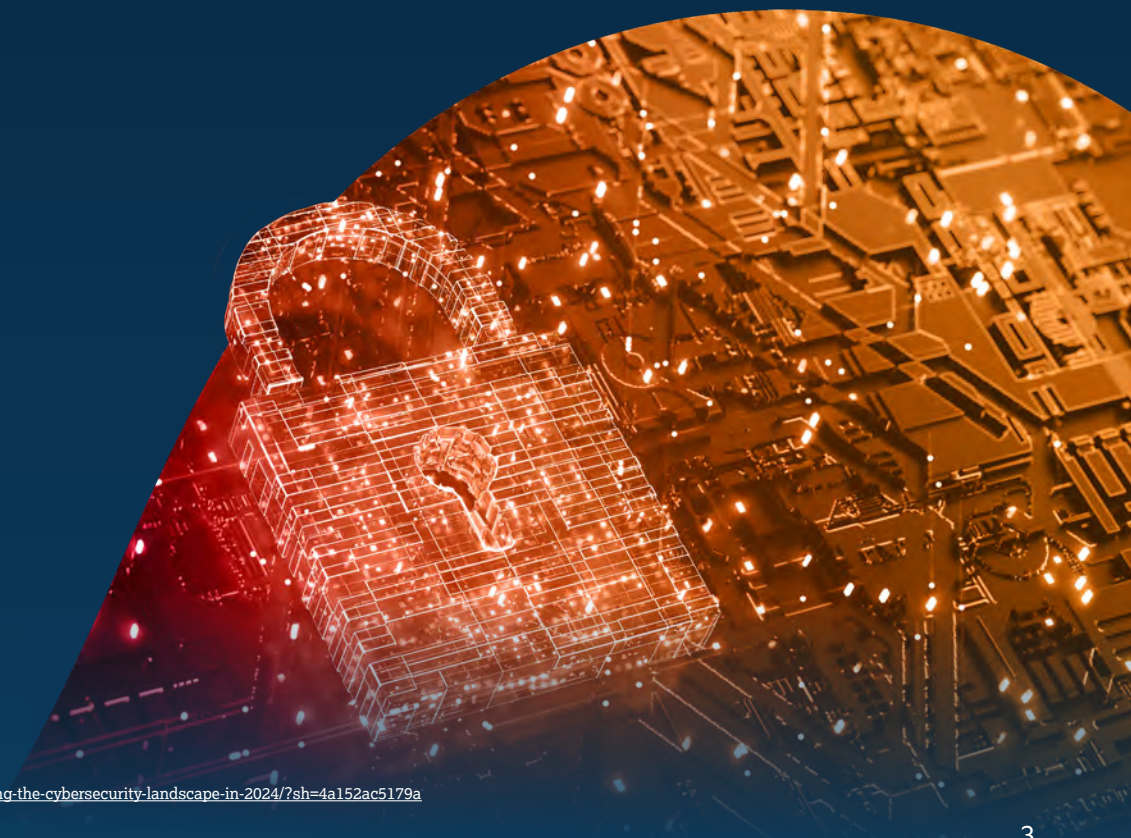
人工知能 (AI) が発展し、サイバー脅威が急激に複雑化する中、企業も個人も重大なサイバーリスクへの保護対策を大幅に強化する必要に迫られています。攻撃者が短時間で大きな攻撃成果を上げる可能性を高めるものが、より優れたサイバー防御戦略にも貢献しているのです[1]。最近の Splunk の調査結果からのAIに関する発見によると[2]、70%のシニアセキュリティエグゼクティブは、AI が防御者以上に攻撃者に多くのメリットをもたらすと考えており、35% は、サイバー防御でその差をすでに体感しています。

しかし、希望がないわけではありません。最近のゴールドマン・サックスによるレポートでは、生成 AI によって国内総生産 (GDP) が 7% 上昇すると提言しており、単一のテクノロジーとしてはまさに異例の効果と言えます。サイバー犯罪者も生成 AI を利用して標的型攻撃を仕掛けており、攻撃の洗練度と展開速度を高めています。生成 AI を活用することで、攻撃者は標的に合わせてパーソナライズしたフィッシングメールを作成することもできます。完成したメールはスペルミスがなく、文法も正確なので、検知するのは至難の業です。現在利用可能なダークウェブ AI ツール (FraudGPT など) により、攻撃者はソーシャルエンジニアリング向けのより複雑なディープフェイク攻撃を仕掛けることができ、ターゲットの感情や信頼をさらに短時間で操作できます。

ドメインはサイバー攻撃の起点となる基盤

フィッシング攻撃、ビジネスメール詐欺 (BEC)、ソーシャルエンジニアリングがさらに複雑な攻撃 (マルウェアやランサムウェアなど) に発展する中、最高情報セキュリティ責任者 (CISO) が、ドメイン名や外部からの攻撃を受けるオンラインの外壁部分に注意を払わないのは驚くべきことです。CISO は、ネットワークの補強に多くの時間を割いていますが、その周辺は変化しています。自社のドメインレジストラの実体を把握していない CISO は少なくありません。レジストラが適切なエンタープライズレベルのセキュリティを提供しているかどうか把握している CISO はかなり少数です。

ウェブサイト、E メール、認証、VoIP、クライアントポータル、サプライヤーアプリケーションなど、グローバル企業はあらゆるものをインターネットに依存しています。これは、外部からの攻撃を受ける組織の外壁部分であり、サイバー犯罪や不正行為を常にモニタリングする必要があります。サイバーリスクが増大し続ける中、組織やサイバー保険会社は、サイバーリスクを定量化し、損害賠償能力に対処するという、より大きな課題に直面しています。このため、ドメイン名は組織のサイバーセキュリティ体制にとって、まさに欠かせない要素となっています。インターネットとドメイン名は、ビジネスインフラとビジネスの継続性に必須と言えます。



1. forbes.com/sites/emilsayegh/2023/12/19/navigating-the-cybersecurity-landscape-in-2024/?sh=4a152ac5179a
2. splunk.com/en_us/form/ciso-report.html

重要なビジネス機能を支えるドメイン名は、エコシステム内で稼働し、あらゆる組織にとって、外部からの攻撃を受ける外壁部分の一部となっています。こうした環境では、ドメイン名とサブドメインは、文字どおり侵害される（乗っ取られる）か、悪意を持って登録されるリスクがあります。つまり、ブランドによく似たフェイクウェブサイトが、BEC 攻撃やフィッシング、マルウェア配布攻撃など、悪意のある目的のためにブランドになりすますということです。空きがあれば誰でもドメイン名を登録できるという基本的な事実に、多くの人が驚きます。そのため、自社ブランドを使用するドメインの登録を怠ったり、同様の戦略や別の手法で自社ブランドを守らなければ、ブランド名とすでに確立された信用をオンラインで悪用して金儲けをしようと待ち構えている詐欺師の思うつぼです。結果として、自社の収益と名声をともに危険にさらすことになり、当然ながら、消費者の安全に対する懸念も生じます。」

Ihab Shraim、最高技術責任者、
CSC のデジタルブランドサービス（Safety Detectives インタビューより）

組織とそのドメインに対する攻撃方法はいくつかあります。

ドメインの侵害やサブドメインの乗っ取り

サイバー犯罪者は、セキュリティが施されていないあらゆるドメインを侵害します。企業は多層防御アプローチに着手し、こうした侵害に備えるべきです。第一に、ドメインポートフォリオ（買収などによって複数のブランドで構成される場合もあります）とオンラインドメインネームシステム（DNS）フットプリントのセキュリティを確保することで、ブランドのオンライン事業の安全を確保する必要があります。

悪質な不正ドメインを作成

一部の国や地域では、登録商標、登録企業、ローカルプレゼンスの提示を求めることで内線番号での登録を制限していますが、注意すべきは、誰でも任意のドメインを登録できるという点です。こうしたフェイクドメインを登録する目的は、標的とするブランドの消費者の信頼を利用することで、巧妙なフィッシング攻撃、別の形式でのデジタルブランドの乱用、知的財産（IP）の侵害を試みることです。攻撃を受けると、収益の損失、トラフィックのリダイレクト、正規ブランドの評判の失墜につながり、詐欺師の懐を肥やすことになります。フィッシング詐欺師や悪意のある第三者が容易に利用できる、置き換えや類似名を用いたドメインなりすましの手口は無限に存在します。

新たに失効したブランドドメインを第三者が再登録

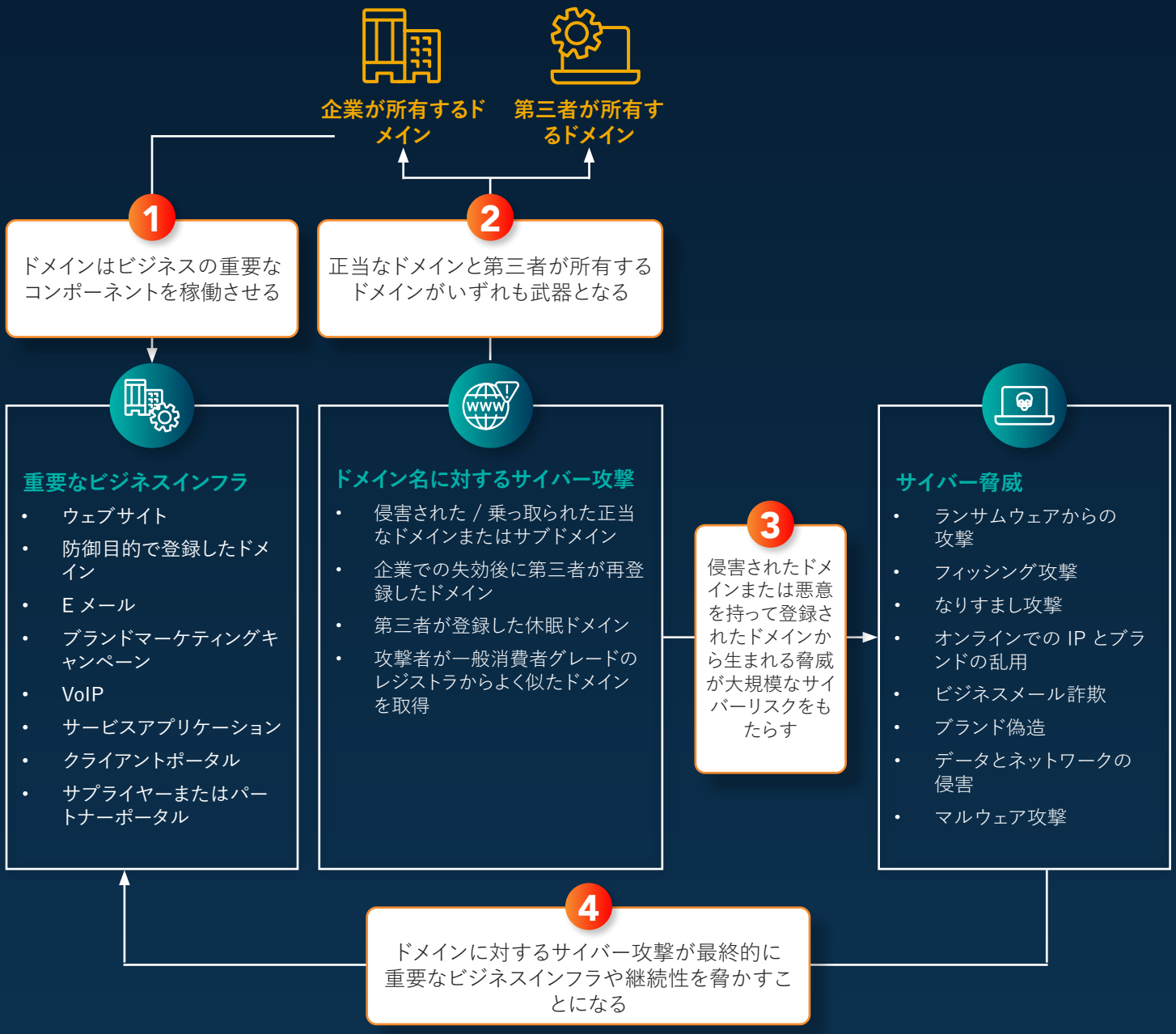
企業は、自社ブランド名を語るオンライン詐欺を防ぐために、非常に重要なドメイン名を登録して自己防衛します。場合によっては、登録後にコストの圧力やブランドの減速に直面し、登録したドメインを失効させることもあります。サイバー犯罪者はこうした事態を虎視眈々と狙っており、失効した同じドメイン名を悪質な目的で即座に再登録します。彼らは、武器として利用できるブランドの空きドメインに常に注目しています。

休眠ドメイン

サイバー犯罪者によっては、登録したブランドのドメインをそのまま保有することがあります。おそらく、ホールディングページやパーキングページをホストするか、「サイト準備中」というメッセージを掲げて、標的となる組織にドメインを再び売却する機会を狙っているのです。また、フィッシング攻撃やマルウェア攻撃など、さらに大規模で悪質な活動を計画している可能性もあります。最初の登録日から 6 か月以上経ってから悪質な目的で活用される休眠ドメイン名は、「サブマリンドメイン」と呼ばれます。休眠ドメインは多くの場合、初期検知を回避します。通常はレッドフラグが上がるはずのアクティブな MX レコードなど、攻撃のために登録されたドメインの特徴をすぐには発揮しないからです。この大きな間隙を活かして、サイバー犯罪者はより複雑でパーソナライズされた攻撃キャンペーンを構築し、さらに破壊的な結果をもたらします。

ドメインの年数にかかわらず、ドメインの登録が以前識別された脅威とどのくらい近いのか常に監視し、登録パターンの有無を確認することも重要です。登録パターンを 一箇所で特定するのは容易ではありません。しかし、ドメインレジストラが独自のデータとさまざまなトップレベルドメイン（TLD）に AI と機械学習テクノロジーを導入していれば、IP アドレス全体でパターンを特定できます。ドメインアクティビティにおける模倣行動を監視することも重要です。つまり、ブランドが新しい製品やサービスに合わせて一連の新しいドメインを登録した場合に、第三者も同じようにしているかどうか確認します。

ドメインの外部攻撃サーフェス



データ流出を防ぐ重要性、ID と脆弱性の管理、アクセス制御、データ保護、クレデンシャル情報の盗難、ソーシャルエンジニアリング戦術に常に用心する必要性など、サイバーセキュリティのほとんどのリスクは、ビジネスリーダーにとって共通の認識と言えます。しかし、日々のサイバーセキュリティ保護を見ると、多くのチームが組織のドメインセキュリティを誰が担当しているのか把握していないことは明らかです。ドメイン名は、マーケティングやブランドのイニシアチブで頻繁に使用されるため、セキュリティチームは、マーケティング部門や法務部門に属するオンラインドメイン名を保護しているような感覚になるかもしれません。組織がドメインレジストラの実体を把握していない場合、レジストラが使用しているポリシーや、ブランドの商標を使用したドメインに導入されたセキュリティ対策を把握していないという可能性が生じます。

残念ながら、攻撃者はビジネスのオンラインプレゼンスの成長をひそかに追跡しており、野放し状態の企業ドメイン名を標的にすることで、格段のメリットを得ることになります。組織のセキュリティ体制を強化しないと、いずれ大惨事に巻き込まれることになります。ドメイン攻撃および DNS 攻撃に悩まされ、金銭的な損失や評判の失墜といったリスクにさらされるおそれがあります。先日、CSC のドメインセキュリティレポートでは、Forbes のグローバル 2000 リストの企業を調査しましたが、4 分の 3 近くの企業は、ドメインセキュリティ対策を 50% 未満しか導入していません。この結果とともに、多くの組織がドメインレジストラについて把握していないという事実を考慮すると、ドメインセキュリティは後回しにされる傾向があることを示唆しています。社内のオーナーシップに欠けていることもその原因の 1 つでしょう。

エンタープライズクラスのレジストラと提携する価値

ドメインレジストラは、大きく 2 つのカテゴリーに分けることができます。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です。一般消費者グレードのレジストラは、全世界のすべてのレジストラの 99% 以上を占めます。個人や起業家向け、または事業を始めたばかりのスタートアップ企業のドメインサービス、ウェブサイト、E メールに対応しています。エンタープライズクラスのレジストラは、ドメインおよび DNS 管理、セキュリティ、ブランド保護 / 詐欺対策、データガバナンス、サイバーセキュリティに関して、高度なビジネス能力、専門知識、サポートスタッフを求める企業やブランドオーナーとの連携を専門にしています。

一般消費者グレードとエンタープライズクラスの比較

一般消費者グレードのレジストラ	エンタープライズクラスのレジストラ
一般消費者グレードのレジストラは、個人や起業家、事業を始めたばかりの小規模事業者向けにドメインやウェブサイト、E メールのサービスを提供します。	エンタープライズクラスのレジストラは、ドメインおよびドメインネームシステム (DNS) 管理、セキュリティ、ブランド保護 / 詐欺対策、データガバナンス、サイバーセキュリティに関して、高度なビジネス慣行、能力、専門知識、サポートスタッフを求める企業やブランドオーナーとの連携を専門にしています。

エンタープライズクラスのレジストラのセキュリティ対策は万全

- ICANN およびレジストリ認定済み
- すべてのドメイン、DNS、デジタル証明書プロバイダーの完全なアカウンティング
- 書面による申請が必須 (電話不可)
- データおよび一般データ保護規則 (GDPR) への準拠
- レジストリ移転ロックポリシー

- ISO 27001 認定データセンター
- SOC 2® コンプライアンス
- 第三者の侵入テストと脆弱性テスト
- 規制セキュリティテスト (SQL インジェクション、XSS など)

- 本人確認 (KYC) ID 認証
- 外国資産管理室 (OFAC) によるスクリーニング
- 全世界 24 時間 365 日の現地言語での社内サポート
- サイバーセキュリティスタッフを定期的にトレーニング

ベストプラクティスとなるのは、人材、プロセス、テクノロジーに投資し、セキュリティを重視しているエンタープライズクラスのプロバイダーを利用することでしょう。そうしたプロバイダーが、今日のグローバル企業のニーズを満たすサービスを提供しているのは明白ですが、企業側には、サードパーティプロバイダー間の違いを把握しなければならないという課題があります。コンプライアンスやリスクの懸念とともに、選択したプロバイダーが、組織の全体的なセキュリティ体制に関する判断にどの程度フィットするのか把握する必要があります。

ドメインポートフォリオのセキュリティを確保するためにエンタープライズクラスのレジストラに求められる 7 つのステップ

デジタル証明書ポートフォリオの管理のように、ドメイン名の管理は複雑になりがちです。以下のステップに従うことで、重要な企業資産を管理し、ブランドに対するセキュリティ脅威を軽減できます。

1

公開鍵インフラ (PKI) でデジタル証明書を管理するように、ドメイン名のグローバルポートフォリオを単一の管理システムで管理することで、一貫したプロセスを確立し、企業が信頼する資産のセキュリティを確保できます。

一元化

2

すべてのドメイン資産を一元化することで、デジタル証明書の管理と同様に、多くのアプリケーションプログラミングインターフェース (API) を利用して自動化を進めることができます。ドメインポートフォリオ API には、以下のようなオプションが求められます。

- メインポートフォリオのレポート
- 新たな登録に向けたドメインの空き状況チェック
- オーダーテンプレート機能を使用するドメイン登録 (幅広い拡張子の登録を完了)
- ネームサーバーと WHOIS 連絡先のアップデート
- 名前の DNS レコードの検索と変更
- URL 転送管理
- ドメイン上のセキュリティ関連イベント 10 種類に関するレポート (監査、またはセキュリティ情報イベント管理サービスプロバイダー (SIEM) の統合用)
- デジタル証明書管理 (証明書のオーダー、更新、検索、再発行、無効化など。オーダーとアップデートに関するすべてのアクションにステータスチェックを利用できます)

自動化

3

それぞれのドメイン名に対応する、さまざまな管轄地域を把握しているプロバイダーを利用することで、時間を節約することができ、データを常に最新の状態に保ち、国や地域の規則に従って運用できます。

コンプライアンス

4

ドメイン名と DNS を統合し、すばやく安全に変更できる体制を整えることが非常に重要です

統合

5

同じ企業は存在しないため、それぞれに異なるセットアップが必要です。つまり、ドメインは非常に分散的に使用されているか、ビジネス単位ごとにセグメント化されているのかを意味します。多種多様なグループで管理できるシステムを確立するには、適切なユーザーが適切な情報にアクセスできるように、一定の対応力が求められます。さらに、企業はドメインポートフォリオの複雑なデータを操作し、理解しなければなりません。ビジネスは、膨大な量のデータを分析し、データに基づいて判断を下せるように、安全で信頼できる、豊富な機能を備えた環境ですばやくデータにアクセスする必要があります。定期的に確認すべきレポートには、以下のものがあります。

- ライブサイトステータス – ドメインがコンテンツを解決しているかどうかを可視化
- ブランド文字列カウント – ポートフォリオ内でブランドがどのように示されているかの分析情報
- 国 – ブランドのグローバルプレゼンスがどのように使われているかを把握

柔軟性

6

年々、新規ドメイン名がますます増加する中で、想定される脅威に基づいて、どのドメイン名を登録すべきか適切に判断する必要があります。ブランド保護をサポートする戦略的なアドバイザーチームを編成すると効果的です。以下のような重要な質問の答えを導き出すうえで役立ちます。

- 適切な数のドメインを確保しているか? 防御目的の登録を増やしてリスク緩和を強化すべきか?
- 脅威インテリジェンスによって、ドメインベースの攻撃を緩和する、エンドツーエンドのワークフローを導入しているか?
- ドメインの登録場所を確認するにはどうすればいいのか?
- 登録しないと、どのようなリスクが生じるのか?
- 組織内での情報共有を徹底し、ドメインを一元化的に登録するにはどうすればいいのか?

変化する状況

7

あらゆるバージョンのドメイン名を登録できる企業は存在しません。そのため、効果的なドメイン監視ソリューションを導入することで、ブランド名の利用を試みる第三者を特定できます。

監視

エンタープライズクラスのレジストラと連携することで、EU NIS2 サイバーセキュリティ指令がドメインと DNS にもたらす影響の評価

サービスの内容:

「2024 年 10 月 17 日までに、委員会は、DNS サービスプロバイダー、TLD ネームレジストリ、クラウドコンピテンシーサービスプロバイダー、データセンターサービスプロバイダー、コンテンツ配信ネットワークプロバイダー、マネージドサービスプロバイダー、マネージドセキュリティサービスプロバイダー、オンラインマーケットプレイスのプロバイダー、オンライン検索エンジンおよびソーシャルネットワークサービスプラットフォーム、トラストサービスプロバイダーを対象とした、測定のための技術的・方法論的要件に関する法律を施行します」[3]

成立理由:

「2016 年に導入された EU サイバーセキュリティ規則は、2023 年施行の NIS2 指令で更新されました。高まるデジタル化に対応し、進化するサイバーセキュリティ脅威の状況に適合するために、既存の法律の枠組みの近代化を図る施策でした。サイバーセキュリティ規則の範囲を新たなセクターや法人まで拡大することで、公共機関と民間機関とともに、所轄官庁と EU 全体のレジリエンスとインシデントへの対応能力を改善します」[4]

3. nis-2-directive.com/NIS_2_Directive_Article_21.html#:~:text=By%2017%20October%202024%2C%20the,service%20providers%2C%20content%20delivery%20network
4. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

一般消費者グレードのレジストラを選ぶリスク

企業がコスト削減を図る場合、ドメインポートフォリオの軽量化は容易な目標と見なされがちです。この短期的な対策が、ドメインの長期的なリスクを招きます。攻撃者はドメインを攻撃することで、正当なブランドから収益を吸い上げるなど、多くの影響をもたらします。

ドメインセキュリティは、オンライン環境でブランドを保護するサイバーセキュリティに欠かせない要素です。しかし、一般消費者グレードのレジストラでは、必ずしも最優先の機能ではありません[5]。一般消費者グレードのレジストラはドメインセキュリティを優先していることが多くないため、信頼できるパートナーとは言えません。この信頼の履き違えが、企業の全体的なセキュリティ体制に影響を及ぼします

多くの企業は、すべてのレジストラが同じであると誤解しています。

一般消費者グレードのレジストラは、クライアントとの取引関係は非常に良好ですが、エンタープライズクラスのプロバイダーが提供する、徹底したレビュープロセスに欠けています。これらのレジストラは、ドメインなりすまし攻撃、ドメインおよび DNS 乗っ取り攻撃、サブドメインの強奪、フィッシング攻撃など、あらゆるデジタルリスクを緩和するソリューションを提供しません。また、一般消費者グレードのレジストラの中には、不注意でブランドを傷付ける可能性があるビジネス慣行も見られます。一部のレジストラは、ブランド名や商標を含むドメイン名をドロップキャッチ、オークション、最高入札者に売却するドメインマーケットプレイスを運営しています。また、ドメイン名スピニングや、商標名を含むドメインの登録を促して、タイポスクワットを増加させるといったケースもあります。こうした慣行はビジネスを直接侵害する行為ではありませんが、ブランドの乱用を助長し、不正な用途で使用されかねない紛らわしいドメインの登録を促しています。

「強さは一番弱いリンクで決まる」という言葉を聞いたことがあるでしょう。あらゆるビジネスは一連のサプライヤーとベンダーを利用していますが、その複雑な一連のベンダーとワークフローが、サプライチェーン攻撃のリスクを高めることになります。サプライチェーン攻撃とは、システムとデータにアクセスできるサードパーティパートナーを通じて、攻撃者がブランドのシステムを侵害するサイバー攻撃です。通常は、サイバーセキュリティ体制が非常に弱いベンダーが標的になります。

プロバイダーに対する攻撃も、ブランドに影響します。この 2 年間にも、注目すべきサプライチェーン攻撃がいくつか発生しています。ビジネスを問わず、安全で、侵害されるリスクのないドメインレジストラを選ぶことが重要です。ドメインレジストラは、企業の全体的なセキュリティ体制で、ドメインレジストラが果たす役割を十分に理解しているチームが吟味する必要があります。ベンダーの侵害記録を監視することが重要です。セキュリティを重視しているドメインレジストラは、最終的にセキュリティチームにかかる負担を一部軽減し、ブランドに多大な損害をもたらす前にドメインの脅威を察知できるようにサポートします。

「2022 年 2 月 16 日公開の年次報告書で説明しているように、当社は 2020 年から同じサイバー攻撃者に年 1 回のペースで侵害を受けました。直近では 12 月に発生しています。ちなみに、初期のサイバー侵入の被害も受けています。GoDaddy® の影響もさることながら、さらに重要なのは、この侵害によって会社の 100 万人以上のユーザーもデータ侵害を受けた点です。」[6]

-- Dark Reading、「What GoDaddy's Years-Long Breach Means for Millions of Clients (GoDaddy の 1 年に及ぶ侵害によって数百万のクライアントに起きたこと)」

5. cpomagazine.com/cyber-security/the-glaring-gap-in-your-cybersecurity-posture-domain-security/
6. darkreading.com/cyber-risk/what-godaddy-years-long-breach-means-millions-clients

侵害された正当なドメインのリスクを多層防御戦略で緩和

サイバー攻撃のリスクを緩和するには、多層防御の原則をドメインセキュリティに適用することです。多層防御アプローチは、標的となる資産を保護するための軍隊の戦略に端を発します。ドメインセキュリティについては、多層型のセキュリティ対策を組織的に活用します。

プロバイダーが、今日のグローバル企業のニーズを満たすサービスを提供しているのは明白ですが、各企業は時間をかけてサードパーティプロバイダー間の違いを把握しなければなりません。IP の侵害や商標法に関する懸念とともに、選択したプロバイダーが組織の全体的なセキュリティ体制に関する判断にどの程度フィットするのか把握する必要があります。

1

エンタープライズクラスのドメインレジストラを確保

ドメインエコシステムについては、フィッシング攻撃、オンライン詐欺、ブランドの乱用とともに、ドメインレジストラの選択が、サイバーセキュリティと IT、法務（総合弁護士）、リスク、コンプライアンス（最高リスク責任者）を担当する人員に影響します。企業のドメインポートフォリオを管理するには、自社システムの保護に投資してきたプロバイダーと連携する必要があります。

2

ドメイン管理プラットフォームへの安全なアクセスを提供するレジストラのみと連携

ドメインセキュリティにおける多層防御アプローチの 2 つ目の階層は、ドメインおよび DNS 管理システムへの安全なアクセスをレジストラに義務付けることです。レジストラは、すべてのクライアントに対して二要素認証を求める必要があります。さらに、IP 認証とフェデレーション ID も提供することで、クライアントは、ネットワークにログインし、安全な認証を経てドメイン管理プラットフォームにアクセスしていることを確認できます。

3

すべてのユーザー権限を確実に制御・管理する

レジストラと連携する際は、権限を細かく制御することが不可欠です。レジストラは、ユーザーアクセスと権限を管理するためにアクセスを許可する必要があります。変更があった場合の通知も含めて、階層型の権限を可視化します。これは、サイバー攻撃が実際にあった場合に特に重要です。攻撃者が登録システムへのアクセスを取得すると、損害をもたらすために新規ユーザーを作成するか、既存のユーザーの権限を変更するからです。

4

高度なドメインセキュリティ機能を使用する

多層防御アプローチの 4 つ目の階層は、個々のドメインレベルで高度なセキュリティ機能を適用することです。適切なドメイン名が決まったら、そのドメイン名に適切な制御を適用しましょう。まずは、レジストリロックを適用します。レジストリレベルでドメイン名をロックできるため、レジストラとレジストリ間の自動化が無効になります。この場合、手動パスワードなしでは DNS を変更できなくなります。正規の担当者がパスワードを確認した上で、ドメイン名のロックを解除するからです。適切な認証なしでは重要なドメイン名の DNS を変更できないため、非常に安全で効果的な方法と言えます。

ハッキングされないまま、正当なサブドメインが乗っ取られる仕組みとは?

さまざまなブランドポートフォリオを保有し、国際的に事業を展開している大きな組織は、世界中に分散した自社のデジタルフットプリントの規模を把握していません。デジタルレコードは時間とともに蓄積するため、サイバーハイジーンが現実的な課題となります。企業は新たな技術へのアクセスをクラウドプロバイダーに頼ってきました。その結果、DNS レコードが増加し、環境もますます複雑になり、ますます高くなるリスクレベルに直面することになります。デジタルレコードを適切に管理せず、日常的なモニタリングを実践しない場合、組織は「ノイズ」を蓄積することになります。シンプルなサイバーハイジーンが複雑になり、サイバー犯罪者に容易に悪用される状況になります。

「デジタルレコードは時間とともに蓄積し、各ドメインの履歴を把握していない管理者は、重要なインフラへの紐づけを懸念するあまり、古いレコードの削除をためらいます。その結果、存在しないコンテンツを指し示す非アクティブな DNS ゾーンレコードが蓄積します。これは「ダングリング (未解決) DNS」と呼ばれ、サブドメインの乗っ取りにより、使用されていない正規のサブドメインの制御を攻撃者が獲得して、独自の詐欺コンテンツや悪質なコンテンツを運営するリスクをもたらします。」

Mark Flegg、セキュリティサービス担当グローバルディレクター、SC Media、「How to ensure DNS records don't become a security hazard (DNS レコードをセキュリティハザードにしないために)」

サイバー犯罪者は、クラウドや一般公開サービスなどのインフラをスキャンします。たとえば、ブランドが使用していないウェブサービスにリンクしている DNS ゾーンレコードを検索します。犯罪者は、認証チェックを実行していないクラウドプロバイダーでコンテンツをホストすることで、以前使用されたゾーン宛先をリクエストし、自作の非合法コンテンツをすべてロードしたサブドメインにウェブユーザーを導くことができます。この場合、組織のインフラや第三者のサービスアカウントを侵害することはありません。例えば、ZDNet では、世界的なコンピューティング企業が攻撃者に乗っ取られ、サブドメインでポーカーカジノが行われたケースを報告しています。

ダンブリング DNS レコードが利用されて、フィッシング攻撃やマルウェア配布攻撃などの他のサイバー攻撃の入り口となり、収益の損失、データ漏えい、消費者の信頼の喪失、セキュリティ侵害によるブランドイメージの低下を招きます。調査を実施したオーストリアの IT セキュリティコンサル会社 Certitude Consulting は、先日公開した「Security Week」で、数千に及ぶ組織や法人はこうした攻撃に対して脆弱だと警告しています。DNS レコードの管理を日常的なサイバーハイジーン慣行の一部とする必要があります。20 年以上にわたり、企業は管理不備のリスクを抱えています。異なるオーナー、ポリシー、ベンダーを利用して DNS を管理していることが原因で、合併買収が発生すると状況はさらに複雑になります。この場合、所有者が明確に把握していないものを削除してしまうという内在的な不安もあります。

CSC のサブドメイン乗っ取りの脆弱性レポートでは、44 万を超える DNS レコードを検証した結果、DNS レコードの 21% 超は未解決のコンテンツにリンクしており、サブドメイン乗っ取りに対する多くの企業の脆弱性は依然として放置されていることを明らかにしました。さらに、27 万 7,000 (63%) 超は、「404 not found」や「502 bad gateway」などのエラーステータスコードを示しています。DNS レコードのメンテナンスは、さまざまな所有者、ポリシー、ベンダーが関与してきた長い履歴が理由で、最も頻繁に先送りされてきた作業の 1 つです。デジタルレコードは時間とともに蓄積し、各ドメインの履歴を把握していない管理者は、重要なインフラへの紐づけを懸念するあまり、レガシーレコードの削除をためらいます。ダングリング DNS は、サブドメイン乗っ取りのリスクにさらされています。サブドメイン乗っ取りとは、使用されていない正規のサブドメインの制御を攻撃者が取得し、独自の詐欺コンテンツや悪質なコンテンツを運営することです乗っ取りが発生すると、フィッシング、マルウェア、ランサムウェアのようなサイバー攻撃の入り口となります。

21%

の DNS アクティブサブドメインレコードは未解決であり、サブドメイン乗っ取りに対する企業の脆弱性は依然として存在。

オンラインブランド保護はサイバーセキュリティに不可欠な要素

悪意を持って登録されたドメイン名は、破壊力の大きいダウンロード型のマルウェアを組み込める、完全な標的型のフィッシングや BEC キャンペーンの前段階となることが少なくありません。こうした初期の攻撃を防ぐには、ドメイン状況を評価し、デジタルブランドイニシアチブのこうした業務に対応するチーム間に存在する分断を排除する必要があります。セキュリティチームは、オンラインでドメインとブランドを常に監視し、ブランド名やそのバージョン違いの名称が、詐欺目的でウェブドメインで使用される可能性を減らさなければなりません。

ドメインのセキュリティ確保は、フィッシングを阻止する道筋のスタート地点です。

企業は、よく似たドメインを登録または再登録してそのオンラインブランドになりすまそうとする攻撃者をあぶり出すために、優れた分析情報を必要としています。この分析情報を利用することで、セキュリティインシデントを発生時点で補足して阻止できるようになります。

歴史的に見て、多くの企業は、オンラインで発生する侵害行動の課題の深さと経路の増加を把握していません。企業は、信頼されるブランドを築くために時間と費用を投資していますが、ひとたびオンライン犯罪の被害者になると、すべてが無になります。自社のブランドを守る最善の方法は、オンライン監視とエンフォースメント活動を組み合わせて詐欺コンテンツを削除する、オンラインブランド保護プログラムを導入することです。ブラウザプロバイダー、インターネットサービスプロバイダー (ISP)、他の SIEM との提携を伴う補完的なソリューションは、ネットワーク遮断を使用するなどして、詐欺ウェブサイトをインターネットユーザーから遮断しますが、さらに包括的な手法の構築にも役立ちます。こうした手法を用いて攻撃者の活動を追跡・修正しつつ、安全なドメイン名管理プログラムを並行して活用することで、ブランドオーナーは自らの公式ドメインポートフォリオを管理・保護できます。

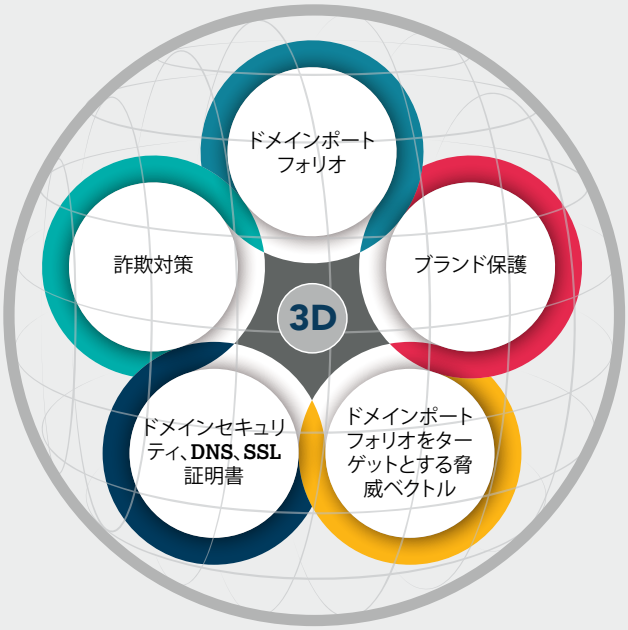
革新的なサイバーリスク低減方法

世界の大手ブランドも採用する、エンタープライズクラスの大手ドメインレジストラである CSC は、ドメイン名エコシステムを変革しています。CSC は、ドメインセキュリティインテリジェンスの効果を確信しています

DomainSec プラットフォーム

DomainSec℠ は、ブランドのドメインエコシステムを保護および防御する業界初の包括的なアプローチです。次世代のオンラインブランド保護機能と詐欺対策機能を備えた、市場で最も革新的な、企業向けのドメイン管理およびセキュリティソリューションです。これらのソリューションのデータを 1 つのプラットフォームに集約することで、CSC は非常に優れたサイバーセキュリティ保護を提供し、

企業のセキュリティ体制を強化できます。CSC は、単なる境界の保護だけでなく、ブランドがゼロトラスト型のセキュリティモデルを改善できるように支援します。業界初のこのプラットフォームは、独自の技術に機械学習、人工知能、クラスタリング技術を組み合わせて、主要な指標を用いて非常にスマートなセキュリティ情報をもたらします。



CSC が提供する防御的および予防的セキュリティ対策のリストをご覧ください。CSC はドメインセキュリティに対して多層防御アプローチを用いることで、お客様のドメインとブランドを保護します。

ドメインセキュリティチェックリストをダウンロード

CSC について

CSC は、セキュリティ脅威の分野で信頼されているインテリジェンスプロバイダーです。ドメインのセキュリティと管理、デジタルブランド保護、詐欺対策を重点領域とし、Forbes 誌の「グローバル 2000」や Interbrand® (インターブランド) が発表する「世界で最も価値の高いブランド 100 社」に名を連ねる企業に選ばれています。グローバル企業がセキュリティ体制に多額の投資をする中、当社の DomainSecSM プラットフォームはサイバーセキュリティの見落としを把握し、オンラインのデジタル資産やブランドを守るのに役立っています。CSC が独自に開発したテクノロジーにより、企業はセキュリティ体制を強化してオンライン資産やブランドの評判を狙うサイバー脅威ベクトルを防ぎ、収益の壊滅的な損失を回避することができます。また、オンラインブランドモニタリングとエンフォースメントアクティビティを組み合わせたオンラインブランド保護サービスも行っています。ファイアウォールの外側で、特定のドメインを狙うさまざまな脅威を多角的に把握できます。フラウド保護サービスは、攻撃の初期段階でフィッシングに対抗できる、当社のソリューションの 1 つです。CSC は、1899 年以来、米国デラウェア州ウィルミントンに本社を置き、米国、カナダ、ヨーロッパ、およびアジア太平洋地域にオフィスを構えています。CSC は、クライアントのロケーションに関わらずビジネス展開ができるグローバル企業であり、当社がサービスを提供する各ビジネスで専門家を採用することにより、これを実現しています。cscdbs.com/jp をご覧ください。

お気軽にお問い合わせください

cscdbs.com/jp