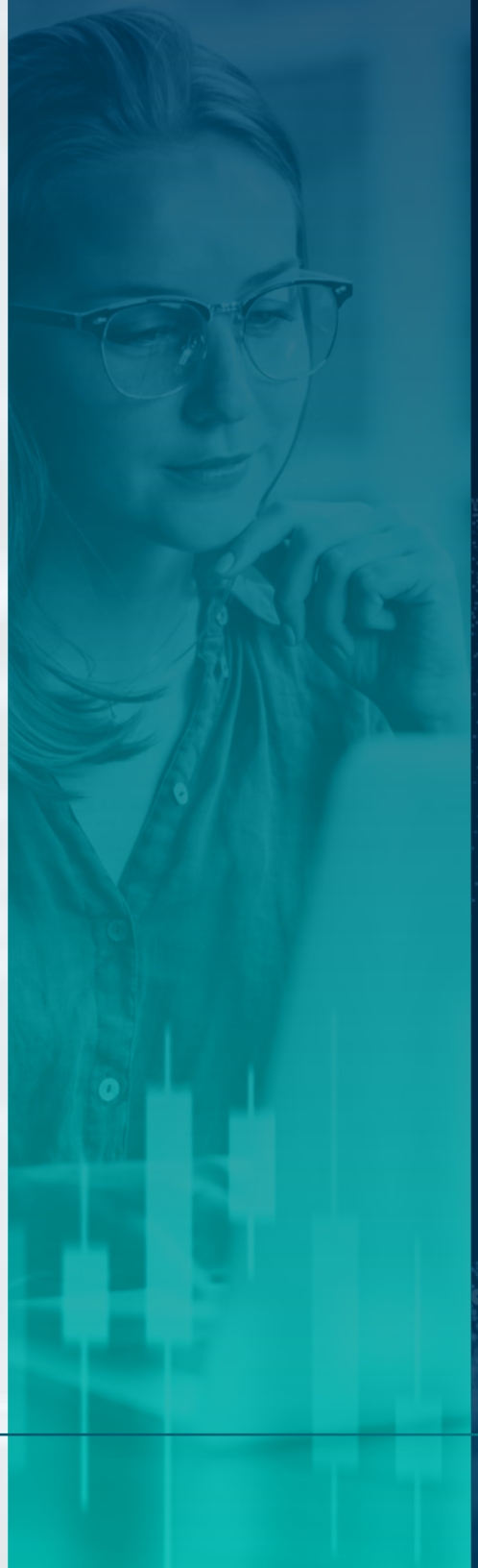
CSC



2023

# ドメイン セキュリティ レポート

CSC は、過去 4 年間、「Forbes グローバル 2000」企業のドメインセキュリティ体制について毎年、最先端の報告を行ってきました。今年は、一部の企業がセキュリティに重点を置くようになりましたが、依然としてかなりのドメインセキュリティリスクを抱えている企業もあります。私たちは、こうした脅威に対する意識を高めて、ドメインセキュリティのベストプラクティスを共有したいと考えています。

「グローバル 2000」企業が、企業のファイヤーウォールの外側にあるドメインエコシステムで発見された、サイバーリスクを軽減するために採用しているドメインセキュリティ対策の状況と、サードパーティによるオンラインブランドの乱用や侵害の可能性を分析しました。

# 主な調査結果の概要

## サードパーティに登録されている .AI ドメインの割合は43%

企業は、自社ブランドの .AI ドメイン名の購入について無関心であるか、そういった企業の代わりに目端の利くオンライン詐欺師にドメインが取られてしまっているのを目の当たりにしています。これは、2023 年に .AI 拡張子が関係するドメイン紛争事例が、前年比 350% 増となったことからも明らかです。

## サブドメインの DNS レコードの 21% 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企業の脆弱性は依然として存在

CSC は、自社データベースの 600 万を超える DNS レコードを分析し、サブドメイン乗っ取りによる侵害の可能性があるクラウドインフラへと導く A レコードと CNAME を確認することで、44 万超の DNS レコードを絞り込みました。

## 「グローバル 2000」企業のブランドに類似した登録ドメイン (紛らわしい文字列) のうち、サードパーティが所有している割合は79%

類似 (フェイク) ドメインの 79% は「グローバル 2000」のブランドオーナー以外のサードパーティが所有するドメインですが、そのうち 40% は今後のフィッシング攻撃で使用される可能性がある MX レコードを保有しています。

## エンタープライズクラスのレジストラ、およびレジストリロックを使用する企業の割合は46%

レジストリロックを導入することで、ドメイン名トランザクションの徹底したセキュリティを実現し、人為的なミスやサードパーティによるリスクを低減することができます。レジストリロックは、偶発的または不正な変更や削除からドメイン名を守ることができる、非常に費用対効果の高い方法です。一般消費者グレードのレジストラを使用している企業のうち、レジストリロックを導入しているのはわずか 7% です。(エンタープライズクラスと一般消費者グレードのレジストラの比較を参照.)

## ドメインセキュリティスコアが0%の企業数は112社

「グローバル 2000」企業のうち 6% は、推奨されるドメインセキュリティ対策を一切導入しておらず、リスクが最も高くなっています。主要なドメインセキュリティ対策の採用状況を分析した結果、セキュリティスコアが 0% の企業では、どの対策も採用されておらず、ドメインセキュリティの脅威のリスクが最も高いことがわかりました。

## DMARC は 6% 成長し、過去 4 年間で最高の伸び率を達成

企業の E メールドメインが、なりすましやフィッシング詐欺に使用されるのを防ぐ目的で設計された E メール検証システムの送信ドメイン認証 (DMARC) の普及率は、2020 年から 28% 増加しました。

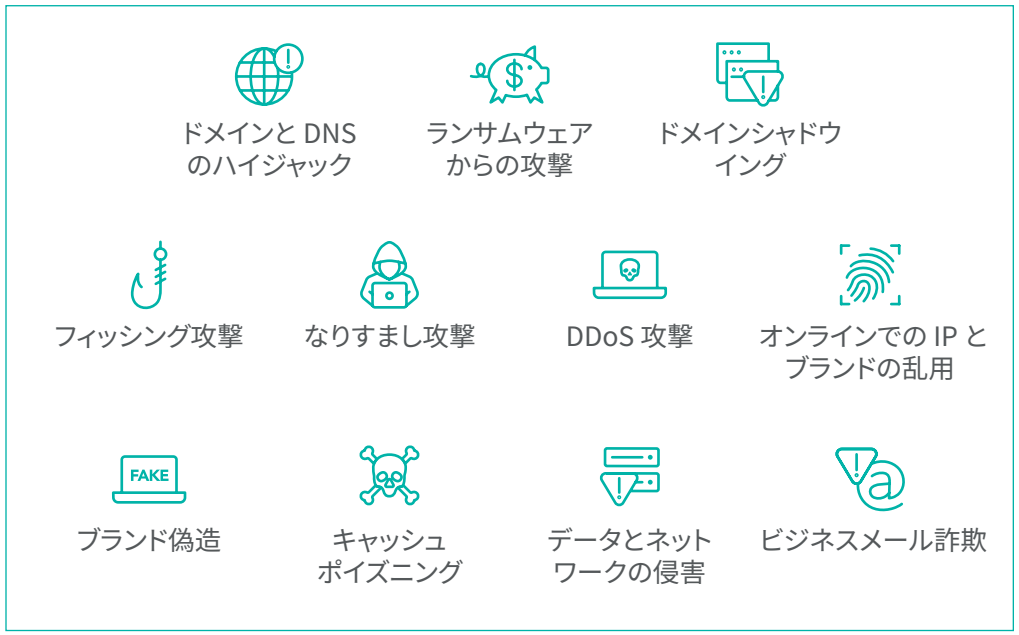
# 2023 年はドメインセキュリティに対する説得力のあるビジネスケースが重視される

サイバーセキュリティの AI 化が進み、攻撃も増加の一途をたどる中、ドメインセキュリティは、企業の最高レベルのサイバーリスク評価における重要な要素となっています。
次の 3 つのドメインセキュリティの脅威から、以下のすべての攻撃が可能になります。

**正規ドメイン名の侵害や乗っ取り**

**紛らわしい文字列などの悪意あるドメイン登録**

**乗っ取りされたサブドメイン**




## ドメインセキュリティの定義

ウェブサイト、E メール、認証、VoIP 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、サイバー犯罪の攻撃やフラウドを常に監視する必要があります。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監視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、リスクを定量化し、損害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。私たちは毎日のように、サプライチェーン攻撃、ランサムウェア、フィッシング攻撃などの新たな動きについて理解し、これらが必要とする対象範囲とこれらを阻止する方法に関して、さらに複雑な階層を追加しています。

CSC は、階層化アプローチでドメインセキュリティを管理します。第 1 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る)、およびオンライン DNS フットプリントを確保することで、ブランドのオンライン事業を確保する必要があります。第 2 に、オンラインブランドを標的とする脅威ベクトルを監視、分析し、権利を行使します。

## サブドメイン乗っ取りとは？

サブドメイン乗っ取りとは、使用されていない正当なサブドメインをサイバー犯罪者が乗っ取り、悪意のあるコンテンツをロードすることで、標的となる企業にフィッシングやマルウェアキャンペーンを仕掛ける攻撃です。攻撃者は、忘れられた DNS レコードを巧みに利用して、自作のコンテンツに導くことで、こうした攻撃を成立させます。

# 新たな脅威:
# サブドメイン乗っ取り

## 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。

CSC は、自社データベースの 600 万を超える DNS レコードを分析し、主要なクラウドインフラへと導く A レコードと CNAME を確認することで、44 万超の DNS アクティブサブドメインレコードを特定しました。このレコードを攻撃者が悪用することで、サブドメイン乗っ取りが発生する可能性があります。当社は、企業のサブドメイン管理の現状を把握し、企業全体のセキュリティ体制への影響を明らかにするために調査を実施しました。

### サブドメイン乗っ取りを積極的に防ぐには

1. 既存の DNS ゾーンファイルを徹底的に監査し、すべてのレコードを確認します。
2. アクティブなドメイン名と対応するサブドメイン名を明らかにします。
3. DNS アクティブレコードを定期的にスキャンして継続的にモニタリングし、何らかのステータス変化を確認したら、年中無休の SOC チームに直ちにアラートを出します。
4. 不正に立ち上げられたサイトに対して直ちに権利行使を実施し、インターネットのブロック機能を使用して有害なオンラインコンテンツを阻止します。

### 実際に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の維持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 レコードがかつてないほど増加し、環境もますます複雑になり、増大するリスク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。

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、自作の正当なコンテンツを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、組織のインフラやサードパーティのサービスアカウントを侵害することはありません。ZDNet では、Microsoft® が攻撃者に乗っ取られ、サブドメインでポーカーカジノを提供されたケースを報告しています。

**このコンテンツにリンクしない非アクティブなゾーンの集合が、いわゆる「ダングリング DNS」となり、企業をサブドメイン乗っ取りのリスクにさらします。**

この「ダンブリング DNS」が、ブランドを標的とするフィッシング攻撃やマルウェア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。調査を実施したウィーンの IT セキュリティコンサル会社 Certitude Consulting は、最近公開した「Security Week」で、数千に及ぶ組織や法人はこれらの攻撃に対して脆弱だと警告しています。

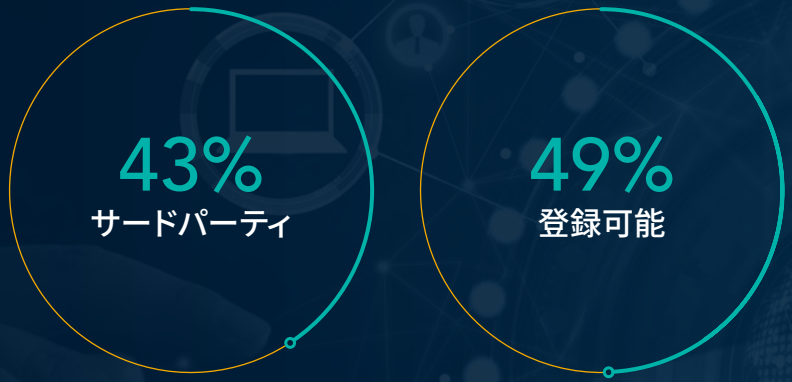
DNS レコードの管理を日常的なサイバーハイジーンの一部とする必要があります。20 年以上にわたり、企業は管理不備のリスクを抱えています。これは企業が異なるオーナー、ポリシー、ベンダーを利用して DNS を管理していることが原因であり、合併買収が発生すると状況はさらに複雑になります。また、所有者が明確に把握していないものを削除してしまうという内在的な不安もあります。

サブドメイン乗っ取りは、ドメインおよび DNS 乗っ取り、ドメインシャドウイング、キャッシュポイズニングなど、現存する多くのドメインセキュリティ脅威の 1 つにすぎません。これらの脅威は、より悪質なフィッシング攻撃やランサムウェア攻撃、ビジネスメール詐欺 (BEC)、データ抽出などのサイバー攻撃を可能にする足がかりになります。

**詳しくは、「サブドメイン乗っ取りの脆弱性レポート」をご覧いただくか、CSC までお問い合わせください。**

# サードパーティに登録されている .AI ドメインの割合は43%

企業は自社ブランドの .AI ドメイン名の購入について無関心であるか、そういった企業の代わりに目端の利くオンライン詐欺師にドメインが取られてしまっているのを目の当たりにしています。




AI テクノロジーの普及により、技術的な状況は著しく変化しています。この変化は、.AI ドメイン名の登録が顕著に増加していることからも明らかで、AI が広く受け入れられ、熱狂的な支持を受けていることがわかります。CSC はこのトレンドの最前線に立ち、クライアントに対して .AIドメインの登録と実施戦略の重要性を積極的にアドバイスしてきました。[1]

また、2023 年には .AI 拡張子が関係するドメイン紛争事件が大幅に増加しています。2023 年 9 月現在、前年に比べて大幅に増加しています。2023 年の前年比 350 % 増という数字と、過去 4 年間の合計件数をすでに上回っているという事実から、警戒と規制の必要性が高まっていることがはっきりとわかります。[2]

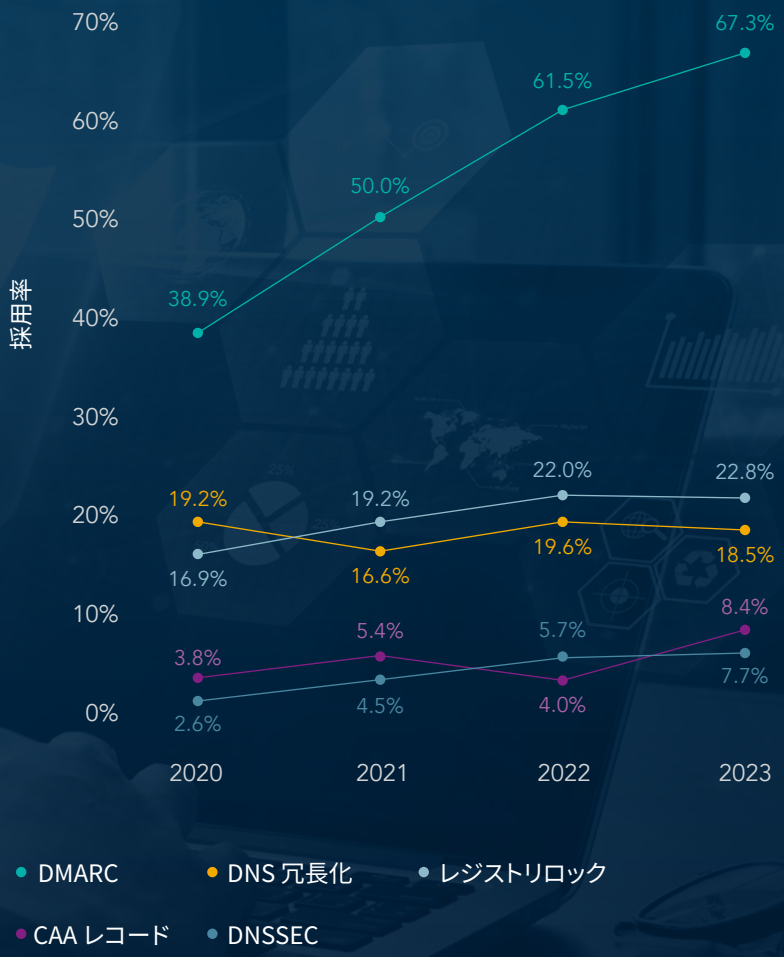
「グローバル 2000」企業の場合、サードパーティによる登録や侵害は全体の 43% です。企業の登録済み .AI ブランドドメインのうち、84% はサードパーティが所有しています。49% はまだ登録可能な状態です。銀行、統合金融、IT ソフトウェアおよびサービスなど一部の業界は、.AI ドメインの取得率が最も高くなっています。

政府が AI ツールに対する規制を強化する一方で、企業は AI システムや AI プロセスの開発、採用を続けています。この傾向は、.AI ドメインの需要がさらに伸びることを示唆しています。さらに、最近になって Google®が .AI ドメインを国別コードではなく gTLD として扱うことを決定しましたが、これは AI の国際市場性が認識されたことを意味します。[3]

.AI ドメイン登録数の伸びは、テクノロジー環境がより広がっていることを示しています。AI が私たちの日常生活のさまざまな状況に浸透するにつれ、それに伴う責任や課題に対処するには、勤勉かつ前向きでなければなりません。

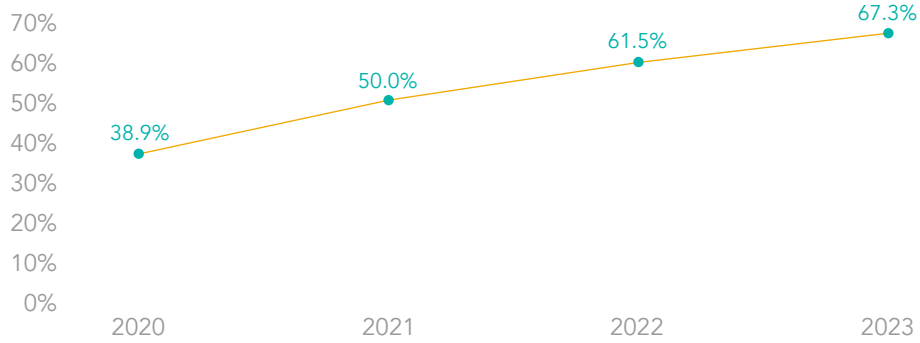
## 今年、.AI 拡張子に関連するドメイン紛争事例は 350% 増加しました。

# ドメインセキュリティ対策の採用動向 (2020 年～2023 年)



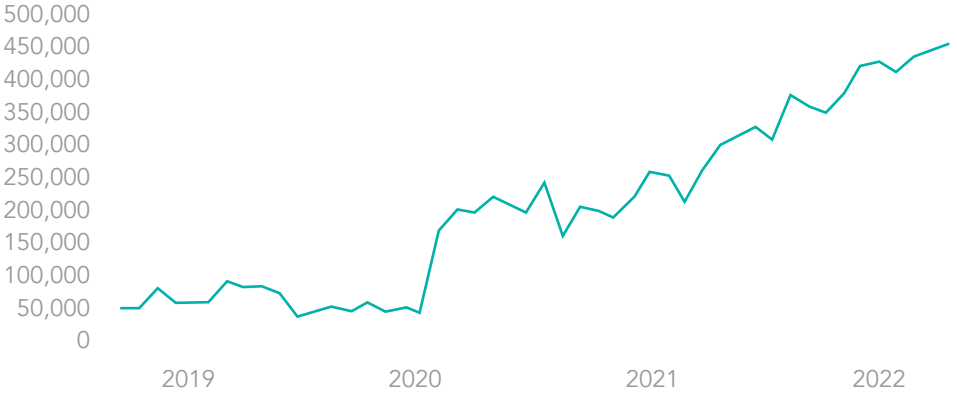

## DMARCの成長は最速

DMARC の使用率が 2020 年の 39% から2023 年には 67% へと急速に上昇したことは、フィッシング攻撃に関するすべてのニュース (その量と複雑さの増大を含む) を考えると、妥当といえるでしょう。




APWG の最新の数字によると、2022 年はフィッシングが過去最高に達した年で、470 万件以上の攻撃が記録されました。また、BEC 攻撃による被害は、2022 年第 4 四半期には平均 132,559 ドルでした。2019 年に入ってからフィッシング攻撃の件数は毎年 150% 増となっています。近年では四半期で 100 万件を超えるフィッシング攻撃があり、毎月約 600 のさまざまなブランドが標的になっています。

## 個別フィッシング攻撃の月間総件数 (APWG)



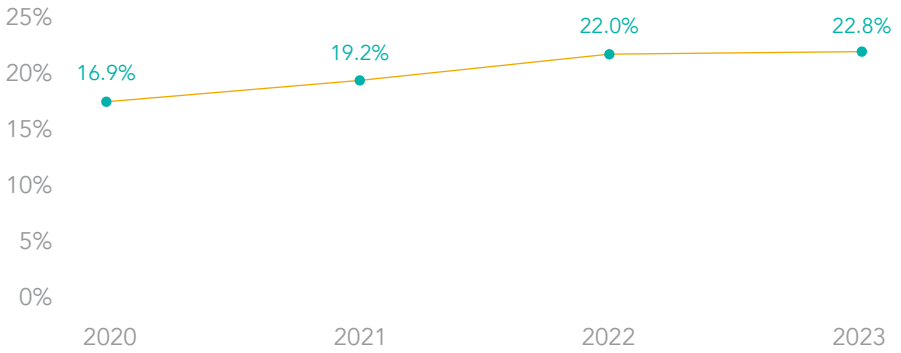

また、認証された E メールに対して、ブランドロゴを表示できるようにする、E メールクライアントのメッセージ識別用のブランド指標 (BIMI) の採用が増加していることも、DMARC の成長の理由です。DMARC は BIMI を設定するためのセキュリティ上の前提条件であり、DMARC と BIMI が連動して、E メールドメイン上の企業のアイデンティティの真正性を検証します。

## レジストリロックは微増、「グローバル 2000」のリスクは高止まり

レジストリロックを有効にしている企業の割合は、2020 年の 17% から 2023 年には 23% に増加しました。また、エンタープライズクラスのレジストラを使用している企業ではレジストリロックの使用率も高く、46% に上りました。政府機関がサイバーセキュリティを強化し、DNS 乱用のリスクを排除するよう圧力を強めている中、規制や業界からの圧力への対応として、ドメイン拡張子のロックを提供するレジストリがますます増えています。レジストリロックを導入することで、ドメイン名トランザクションの徹底したセキュリティを実現し、人為的なミスやサードパーティによるリスクを低減することができます。レジストリロックは、偶発的または不正な変更や削除からドメイン名を守ることができる、非常に費用対効果の高い方法です。しかし、世界中のすべてのレジストリがロックサービスを提供しているわけではなく、ロックできないドメインもあります。

企業のドメインポートフォリオは常に変化しているため、CSC は 20 以上のドメイン名属性を評価する予測モデリングアルゴリズムを使用しています。これにより、特定のドメイン名が企業運営やオンラインブランドにとって業務上不可欠かどうかを特定し、ロックすべき重要なドメインを提案します。

### レジストリロック

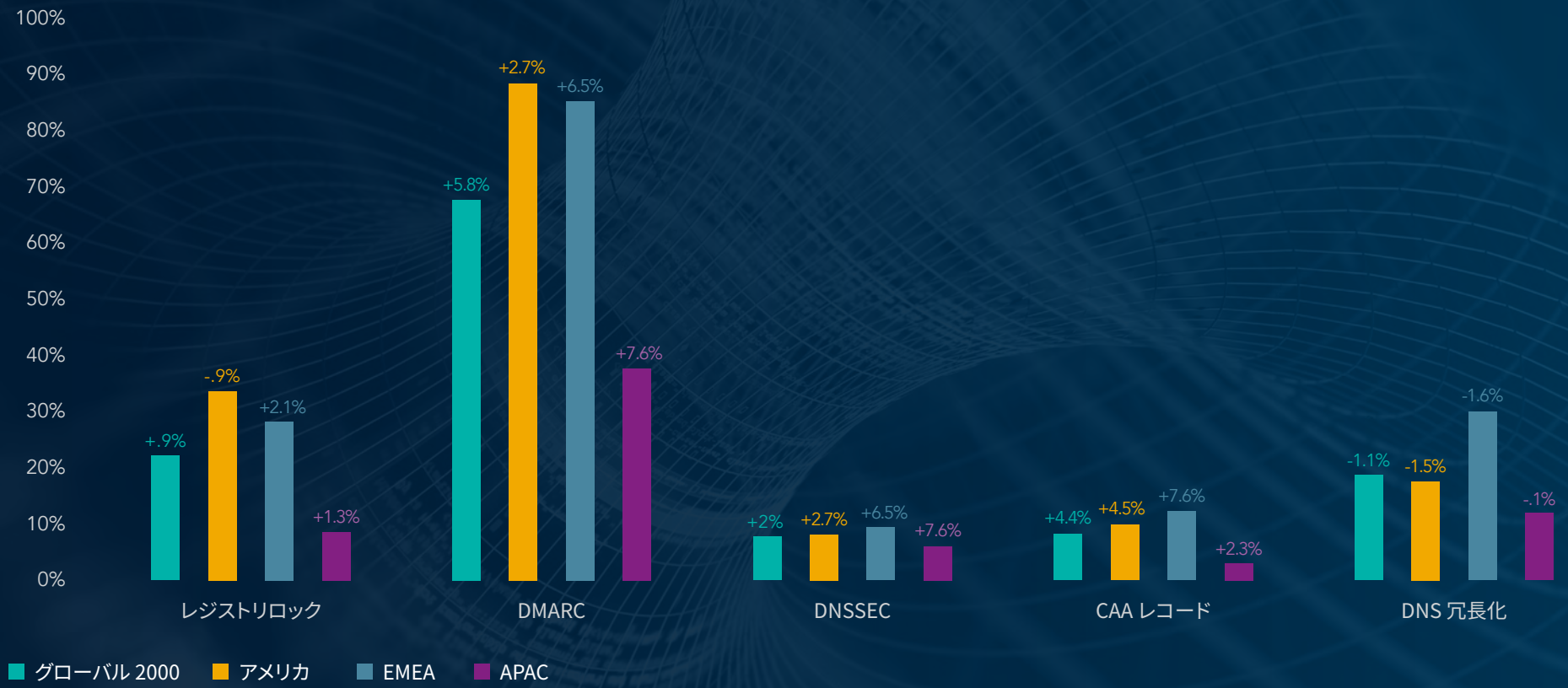


## DNS 冗長化、DNSSEC、CAA レコードなどのセキュリティ対策が一貫していない

DNS セキュリティ拡張 (DNSSEC) を導入している企業はまだ少ないものの、2020 年の 3% から 2023 年には 8% と、過去 3 年間で 2 倍以上に増加しています。DNS の回復力を求める政府機関が増えているにもかかわらず、DNS 冗長化は前年比 1% 減の 19% でした。DNS 冗長化は、どの組織においても中核インフラの重要な要素ですが、このセキュリティ対策の採用は減少傾向にあります。これは企業がコストとリソース割り当ての増加を計画しなければならないためと考えられます。

最後に、CAA レコードの使用は、今年かなり増加し、2020 年の 3.8% から 2023 年には 8.4% へと変化しています。CAA レコードを設定することにより、企業のドメイン名に関する証明書発行者を特定の認証局 (CA) に限定できます。これによって、サイバー犯罪者が指定外の認証局を使って新しい証明書を取得することを防止できます。この場合、リクエストは認められず、企業にアラートが送られます。しかし、ドメイン、DNS、およびセキュアソケットレイヤ (SSL) に複数のプロバイダーを使用する場合は特に、要件を満たすことが難しい場合が多く、多くの企業はまだこのセキュリティ制御を十分に使用できていません。

## 2023 年の地域別ドメインセキュリティ対策



# 2023 年のレジストラタイプ別ドメインセキュリティ対策

このレポートでは、「Global 2000」を構成する企業が使用するドメインレジストラのタイプごとに、ドメインセキュリティの採用動向を分析しました。

### 一般消費者グレードのレジストラ:

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。

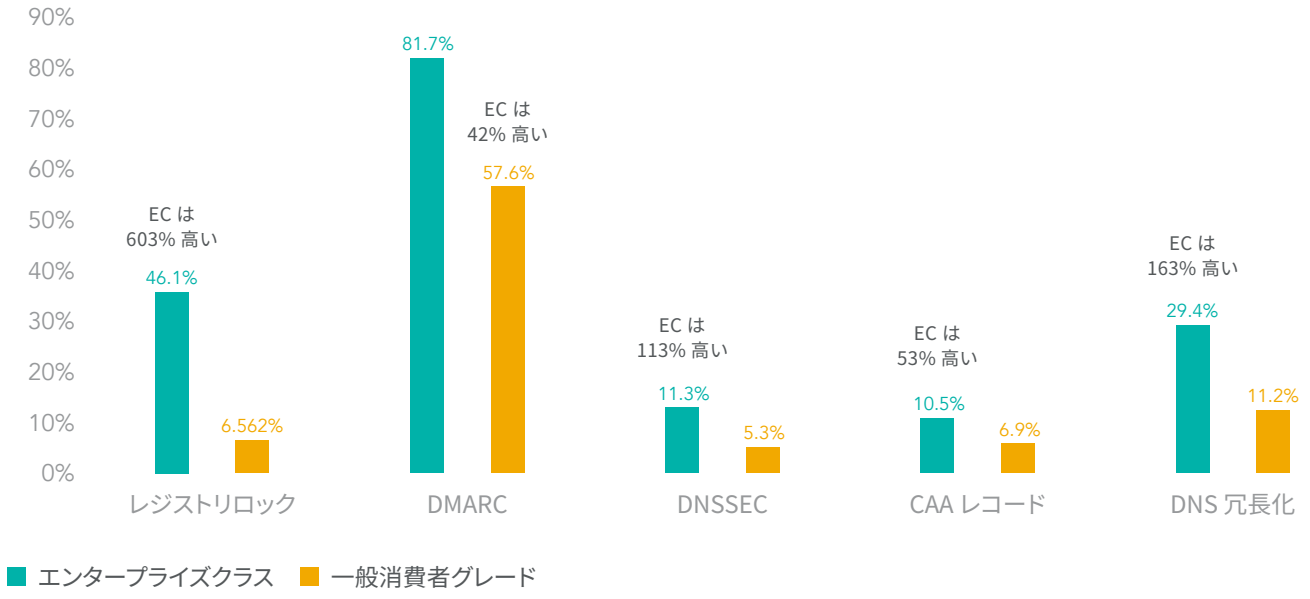
### エンタープライズクラスのレジストラ:

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、フラウド保護、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。

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、企業の全体的なセキュリティ体制に影響を与えうるドメインセキュリティ用に設計されていない可能性がありますが、誤って信頼されています。一般消費者グレードのレジストラのほとんどはレジストリロックに対応していないため、この傾向は特にレジストリロックの採用において顕著になります。

## エンタープライズクラスの機能に依存する企業は、ドメインセキュリティ対策をより多く採用

### セキュリティ対策の熟成度、エンタープライズクラス (EC) と一般消費者グレード (CG) のレジストラ



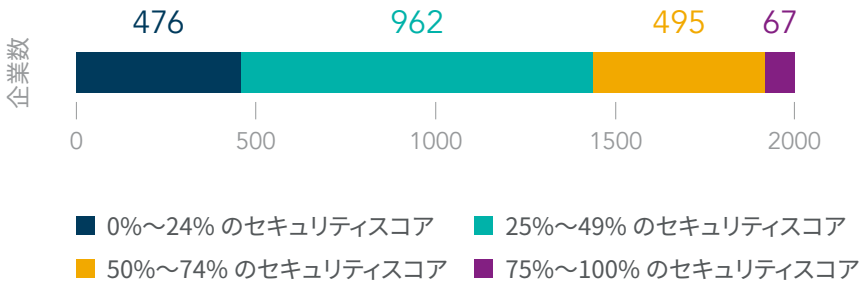
# 全体的なドメインセキュリティ体制

CSC は、企業のドメインセキュリティリスクレベルに応じてグループ化した 8 つの主要なセキュリティ対策の重要性を調べ、各企業の平均スコアを導き出しました。この平均値が企業のセキュリティスコアを構成し、スコアが高いほどセキュリティ体制が強化されていることを示します。つまり、企業はドメインセキュリティの脅威のリスクが低いことを意味します。

## 主なドメインセキュリティ対策:

- エンタープライズクラスのレジストラ
- レジストリロック
- CAA レコード
- DNS 冗長化
- DNSSEC
- SPF
- DKIM
- DMARC

## グローバル 2000」のドメインセキュリティリスクレベル




**全体の 72% の企業が、セキュリティ対策の半分未満しか実施していない**

### スコアが最も高い業界

- IT ソフトウェアおよびサービス
- メディア
- 企業向け製品・サービス提供
- ホテル・飲食・レジャー
- 医療機器・サービス

### スコアが最も高い企業

- ドメインセキュリティ対策を 100% 採用し、最高のセキュリティスコアを獲得した企業は 2 社だけでした。

### スコアが最も低い業界

- 公益事業
- 商社
- 食品市場
- 建設
- マテリアル

### スコアが最も低い企業

- ドメインセキュリティスコアが0の企業は112社。
- これらの企業は主にアジア太平洋地域の企業で、スコアが 0 の企業の 87% を占めています。

# 不審なドメイン、あるいは悪意あるドメインによる「グローバル2000」企業を標的としたアクティビティ

CSC では、「グローバル 2000」企業のブランド名を 6 文字以上含むドメインのうち、ブランド自身が所有していないものを特定し、分析しました。このようなフェイクのドメイン登録は、標的とするブランドへの信頼を利用して、フィッシング攻撃を仕掛けたり、その他さまざまな形のデジタルブランドの乱用や知的財産侵害を起こしたりすることを目的としており、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失墜につながる恐れがあります。

フィッシング詐欺師、また悪意あるサードパーティが利用できるドメインなりすましの手口や置き換えは無限に存在します。

**一般的な紛らわしい文字列は、脅威アクターが使用する最も悪質な攻撃方法の 1 つであるため、当社では意図的に焦点を当てています**

## ドメインなりすましの手法

| | |
|---|---|
| あいまい一致 | cscg1obal.com \| cscgl0bal.com |
| 紛らわしい文字列 – IDN | ćscglobal.com \| csçglobal.com |
| いとこドメイン | cscglobal.jp \| cscglobal.ec |
| キーワード一致 | cscglobalcovid.com \| covidcscglobal.ar \| covid19.com |
| 同音異義語 (soundex) | siesiglobal.com \| cscclobol.com |

## .COM ドメインにおける一般的な紛らわしい文字列 (あいまい一致)

フィッシングドメインで頻繁に検出されるため、よくあるアルファベット置き換えも対象に分析しました。C0rnpanyNarne.com を CompanyName.com のように見せかけるのがその例です。

C0rnpanyNarne.com

**よくあるアルファベット置き換え**

i → l　m → rn　i → l　s → 5　o → 0

e → 3　l → 1　l → i　w → vv

## 類似ドメインの 79% 以上はサードパーティが所有しています。

**サードパーティ所有ドメインのうち:**

**87%** WHOIS または所有権の詳細が非表示となっている割合は、2022 年の 82% に対し、2023 年は 87% でした。増加の原因としては、意図的なもの、GDPR などのプライバシーポリシーに基づく編集によるものなどが考えられます。しかし、特にサードパーティのドメインでは、所有権やアイデンティティを非表示にしたり、隠したりするということは、不正な意図を持った登録の傾向を示しています。

2023 年には **40%** が MX レコードを所有しています。これは、2022 年の 48% に匹敵します。MX レコードは、フィッシングメールの送信やメール傍受に利用できます。

### サードパーティのドメインはどのように使用されていますか?

**36%** 広告やペイパークリックの広告を示すか、ドメインパーキングに利用されている割合

**49%** 非アクティブなウェブサイトを所有していた割合

**1%** ブランドの評判を失墜させお客様の信頼を損ねる恐れがある、悪意あるコンテンツを指していた割合

**14%** ブランド所有者に関連しないライブウェブサイトに転換される割合.

**2023 年 7 月にインスタグラムが Threads を立ち上げたことで、ブランドはすでにサードパーティドメイン登録の影響を感じています。登録されたものの中には提携の主張、ロゴの乱用、ブランドのなりすましなどに使われているものもあります。**

**続きを読む:** CSC の新たな調査によると、インスタグラムが立ち上げた Threads は、すでにフラウドやブランドの乱用の標的として広がりを見せている

# 疑わしいドメインおよび悪意あるドメイン: 標的となっているのは誰でしょうか?

| 業界 | フェイクドメインの脅威が全体に占める割合 |
|---|---|
| 銀行 | 13.1% |
| 建設 | 5.4% |
| 石油およびガス | 4.5% |
| 総合金融 | 4.2% |
| マテリアル | 4.2% |
| IT ソフトウェアおよびサービス | 4.1% |
| 公益事業 | 3.6% |
| 企業向け製品・サービス提供 | 3.5% |
| 保険 | 3.5% |
| 資本財 | 3.4% |
| 耐久消費財 | 3.3% |
| 小売 | 3.2% |
| 化学 | 2.8% |
| 医薬品およびバイオテクノロジー | 2.6% |
| 輸送 | 2.4% |
| テクノロジーハードウェアおよび装置 | 2.2% |
| 食品・飲料・たばこ | 2.1% |
| 通信サービス | 1.9% |
| 医療機器・サービス | 1.9% |
| 半導体 | 1.7% |
| ホテル・飲食・レジャー | 1.2% |
| 航空宇宙および防衛 | 1.1% |
| 家庭用品・個人向け商品 | 1.0% |
| 商社 | 0.9% |
| メディア | 0.9% |
| 食品市場 | 0.8% |

## サードパーティが所有するフェイクドメインの登録に最も関連するドメインレジストラ:

- GoDaddy®
- Namecheap™
- Network Solutions

# 結論

企業がドメインセキュリティに取り組まなければ、そのリスクは壊滅的な結果につながる可能性があります。保護されていないドメインは、サイバーセキュリティ体制、データ保護、消費者の安全、知的財産、サプライチェーン、収益、会社の評判に対する大きな脅威となります。

当社の調査では、「グローバル 2000」企業に関連する .AI ドメインの 43% がサードパーティによって登録されています。.AI 拡張子が関係するドメイン紛争事件が、2023 年には前年比 350% もの増加を見せたことからもわかるように、自社の .AI ドメインを確保しなかった企業は、目端の利く多数のオンライン詐欺師が企業の代わりにこれらのドメインを購入したことに気づき始めています。

企業が戦略的なドメイン登録を補完するには、ゼロトラストフレームワークの中で階層型のセキュリティモデルを使用してドメインセキュリティを適用し、ビジネスへのリスクを最小限に抑えながら、強固な企業セキュリティ体制を構築することが必要です。エンタープライズクラスのレジストラとのパートナーシップは、露出したサーフェス (ドメイン名や DNS など) の可視化と、企業のオンライン事業を標的とした脅威ベクトルの分析機能の獲得のためだけでなく、緩和ソリューションと実施措置を提供するリソースを得るためにも必要です。

**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する >>.**

## CSC の DomainSec プラットフォームについて

CSC の 3D ドメインセキュリティおよびエンフォースメントソリューションは、CSC の DomainSec℠ プラットフォームの機能を利用して構築されました。DomainSec は、CSC が考案した SaaS サイバーセキュリティプラットフォームであり、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。独自の機械学習ディープサーチテクノロジーを使用し、機械学習、AI、クラスタリングテクノロジーを組み合わせて侵害の主要指標を特定します。

DomainSec は、CSC のドメイン管理とドメインセキュリティ、そしてブランド保護とフラウド保護のソリューションを 1 つのプラットフォームで提供します。CSC は、飛躍的に向上した保護機能を提供し、境界の保護にとどまらず、ゼロトラスト型のセキュリティモデルをさらに改善できるよう組織を支援します。

**CSC** は、安全なドメインポートフォリオマネジメント、DNS、デジタル証明書管理、デジタルブランド保護とフラウド保護などの信頼できるセキュリティおよび脅威インテリジェンスプロバイダーとして、Forbes 誌の「グローバル 2000」や「世界で最も価値の高いブランド 100 社®」に名を連ねる多くの企業に選ばれています。グローバル企業は、セキュリティ体制に多額の投資を行い、外部攻撃から保護する努力を続けています。CSC は、企業が自社のドメインセキュリティリスクと、それがゼロトラストモデルとどのように整合するかを理解できるようお手伝いします。CSC が独自に開発した技術により、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から保護し、収益の壊滅的な損失や GDPR のような政策による多額の金銭的ペナルティを回避することができます。また CSC は、デジタル資産保護に向けた包括的なアプローチとして、オンラインの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、さらにはフィッシング対策としてフラウド保護サービスを提供しています。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。

[1]CSC のブログ「AI の準備はできていますか? ポートフォリオに追加するべきドメイン — 誰かが追加してしまう前に」(cscdbs.com/blog/ai-you-ready-a-domain-to-add-to-your-portfoliobefore-someone-else-does/)

[2]DNDisputes.com「AI: Ai拡張子を持つドメイン名紛争例」(dndisputes.com/case/domain/extension/ai/)

[3]Search Engine Land、「Google は今や .AI ドメインを gTLD として扱う」(searchengineland.com/google-now-treats-ai-domains-as-generic-top-level-domains-427770)



CSC10112023