CSC

ドメインセキュリティレポート 2024

はじめに

CSC は、過去 5 年間、「フォーブス・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。企業のファイア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「グローバル 2000」企業が採用しているドメインセキュリティ対策の状況、および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。

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。当社は、これらの脅威に対する意識を評価し、ドメインセキュリティの最善策を共有して、あらゆる組織のドメインセキュリティ体制を強化することを意図しています。

CSC が毎年発行している「ドメインセキュリティレポート」が 、5 周年を迎えるにあたり「フォーブス・グローバル 2000」企業のドメインセキュリティ体制を分析する当社の継続的な取り組みについて振り返ります。今年、CSC は創業 125 周年を迎えるにあたり、当社はデジタル空間における企業周辺の外側に潜むサイバーリスクと、強固なドメインセキュリティ対策の必要性について引き続き意識向上を図ります。

調査結果の概要

医療機器・サービス業界：サイバー攻撃の増加が顕著であるにもかかわらず、ドメインセキュリティのランキングで順位を落とす

今年、業種別のドメインセキュリティで最も顕著な変化が見られたのは医療機器・サービス企業で、2023 年の 5 位から 2024 年には 12 位へと 7 つ順位を下げました。逆に、テクノロジーハードウェア・機器は 2023 年の 13 位から 2024 年には 5 位へと 8 つ順位を上げました。

「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、そのブランドに属していない割合は 80%

「グローバル 2000」ブランドの所有者以外のサードパーティが所有する 80% のホモグリフドメイン（そっくりな偽物のドメイン）のうち、42% が MX レコード（メール交換レコード）を保有しています。（2023 年には 40%） MX レコードは、フィッシングメールの送信やメールの傍受に使用される可能性があります。

「グローバル 2000」企業の 112 社がドメインセキュリティスコアが 0

「グローバル 2000」企業のうち 5% は、推奨されるドメインセキュリティ対策を一切採用しておらず、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。

レジストリロックの利用は 2020 年以降 7% 増加したものの、全体的な普及率は 24% と低水準

レジストリロックを採用することで、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。

2020年以降、DMARC の採用率は 32% 増加

2023 年、Anti-Phishing Working Group (APWG) は、約 500万件にのぼるフィッシング攻撃が記録され、2023 年は最もフィッシングの被害が多い年となったと報告しています。このような攻撃に後押しされ、送信ドメイン認証（DMARC）の普及が増加しました。DMARC は、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です 。

外部攻撃対象領域（アタックサーフェス）は、ドメインエコシステムが存在する場所

サイバー脅威の AI 化が進むにつれ、攻撃は増加の一途をたどっています。このため、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の重要な要素となっており、図 1 に示されているように、真の攻撃脆弱性として企業のドメインエコシステムを含める必要があります。正規ドメイン名の侵害や乗っ取り、または悪意のあるドメイン登録は、図 1 に示されているすべての攻撃を可能にするために使用されます

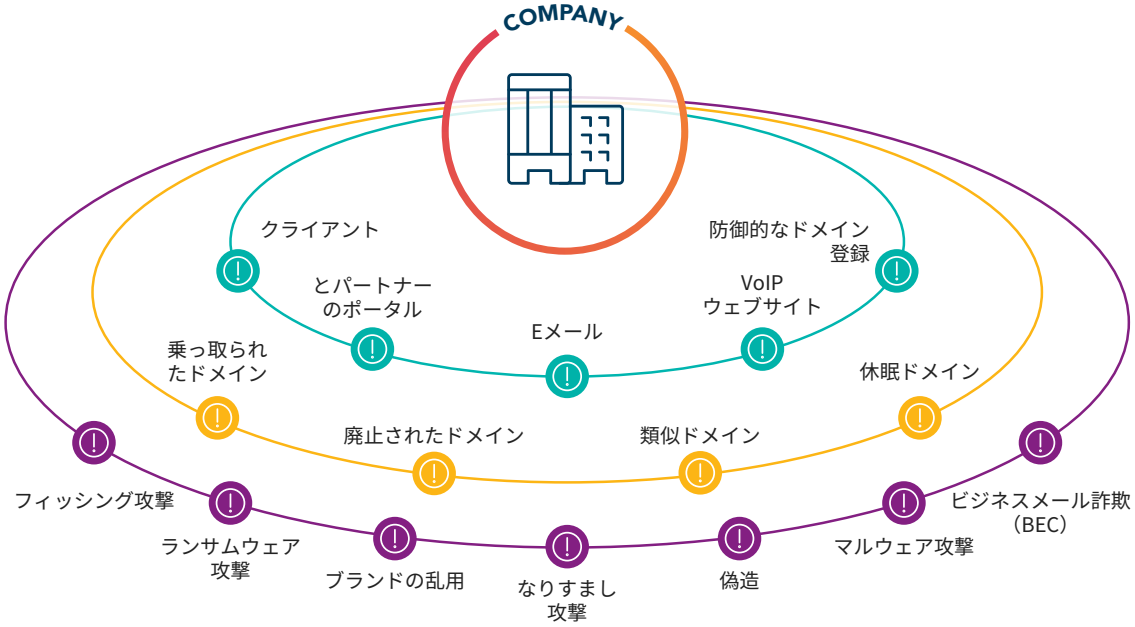
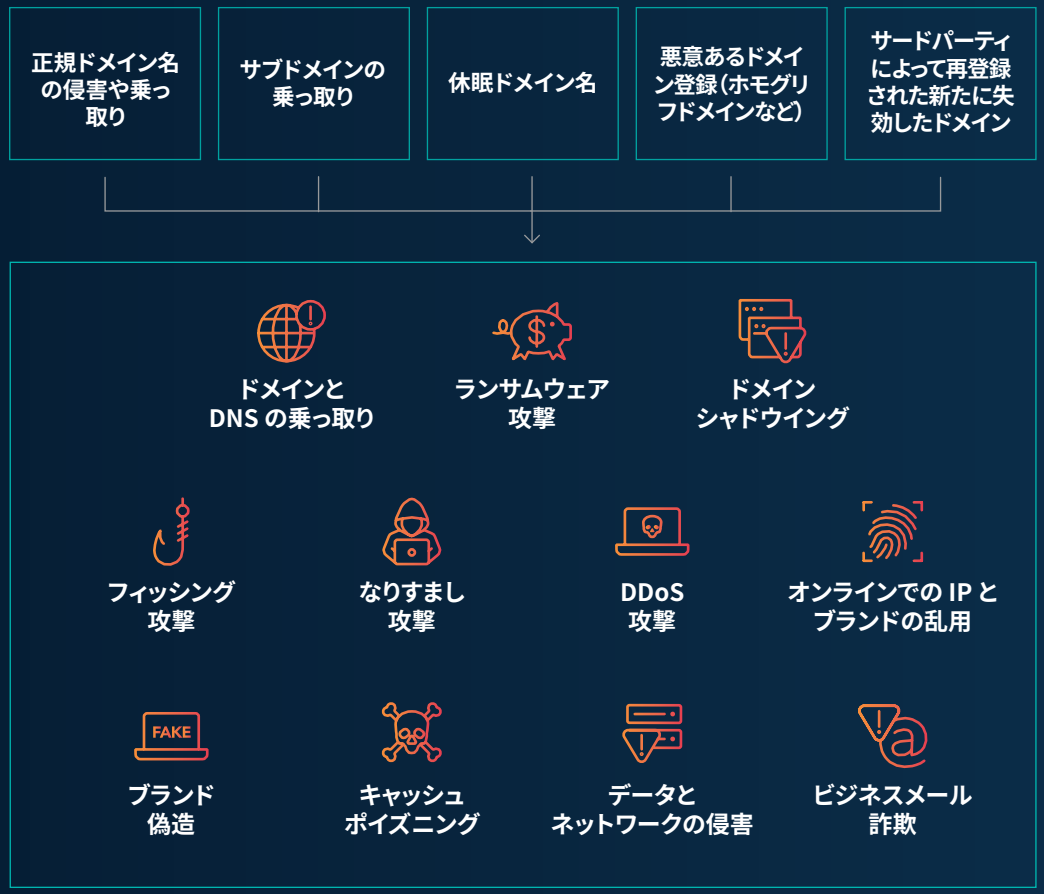


図1：ドメイン名エコシステムの全体図

ドメインセキュリティの定義

グローバル企業は、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、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、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。つまり、インターネットとドメイン名はビジネスのインフラと継続性に不可欠であるため、ドメイン名は組織のサイバーセキュリティ体制の重要な要素であると言えます。



正規ドメイン名の侵害や乗っ取り

サイバー犯罪者は、セキュリティが保護されていないドメインを侵害します。企業は、乗っ取りから身を守るために、階層化された徹底的な防御アプローチから始めるべきです。

サブドメインの乗っ取り

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ホストすることで、標的となる企業にフィッシングやマルウェア攻撃を仕掛ける手法です。これは、忘れられたドメインネームシステム（DNS）（ダングリング DNS）レコードを悪用して、自分たちのコンテンツへ誘導するようにします。

休眠ドメイン名

サイバー犯罪者は、ブランドドメインを登録し、フィッシングやマルウェア攻撃で利用する準備が整うまで休眠させておくことがあります。休眠ドメインは、攻撃を仕掛けるために登録されたドメインであることを示す指標（例えば、アクティブなMXレコードなど）がすぐにはないため、最初の検知を逃れることがよくあります。

悪質なドメイン登録

フィッシング詐欺師や悪質なサードパーティが利用できるドメインスなりすましの文字列やホモグリフは無限にあります。このような偽ドメイン登録の目的は、ターゲットとなるブランドに対する消費者の信頼を利用して、巧妙なフィッシング攻撃やその他の形態のデジタルブランド乱用を仕掛けることです。

新たに失効し、サードパーティによって再登録されたブランドドメイン

企業は、コストの問題から、これまで防衛的に登録されていたドメイン名を失効させることを選択する場合があります。サイバー犯罪者はこれを見計らって、すぐにこれらのドメイン名を悪意のある目的のために再登録します。サイバー犯罪者は利用可能なブランドドメインを常に探しています。

調査結果と分析:「グローバル 2000」のドメインセキュリティ対策の採用動向

CSC は、「グローバル 2000」リスト全体で、5 つの主要なドメインセキュリティ対策、(DMARC、DNS 冗長性、レジストリロック、認証局認可 (CAA) レコード、DNS セキュリティ拡張 (DNSSEC)) の採用状況を調査し、業界グループや地域ごとの採用レベルについて深く分析を行っています。

メインセキュリティ対策の採用動向 (2020 年～2024 年)

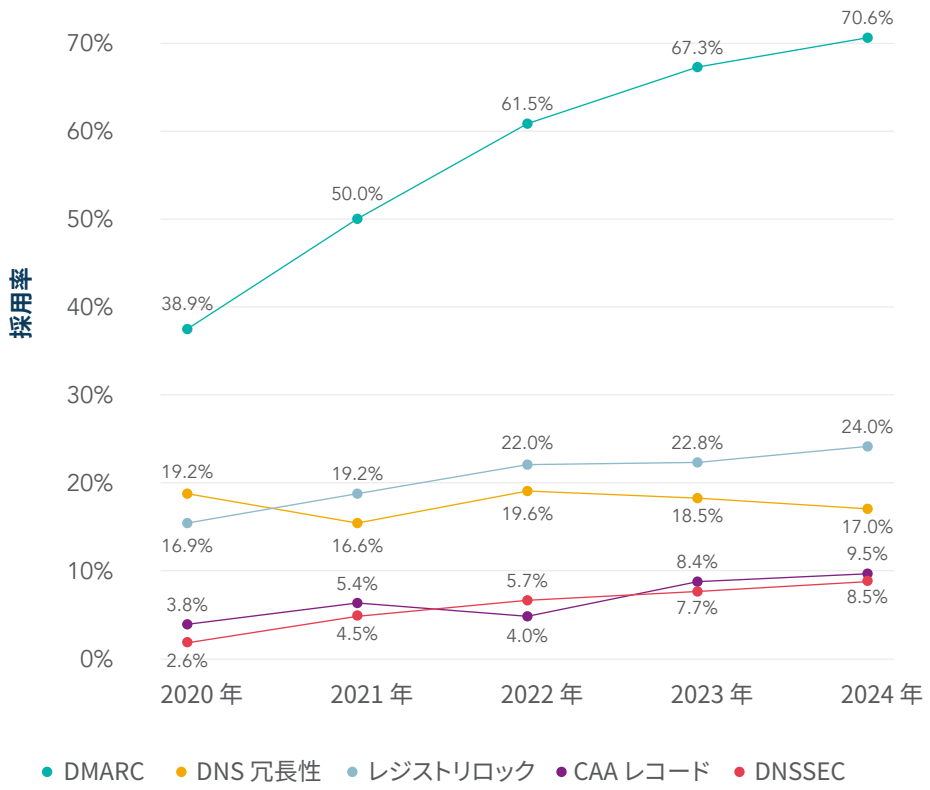


図 2:「グローバル 2000」の 5 主要ドメインセキュリティ対策の採用動向 (2020 年～2024 年)

DMARC の成長が最速

DMARC の使用率が 、2020 年の 39% から2024 年には 71% へと急上昇したことは、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。(図 3)

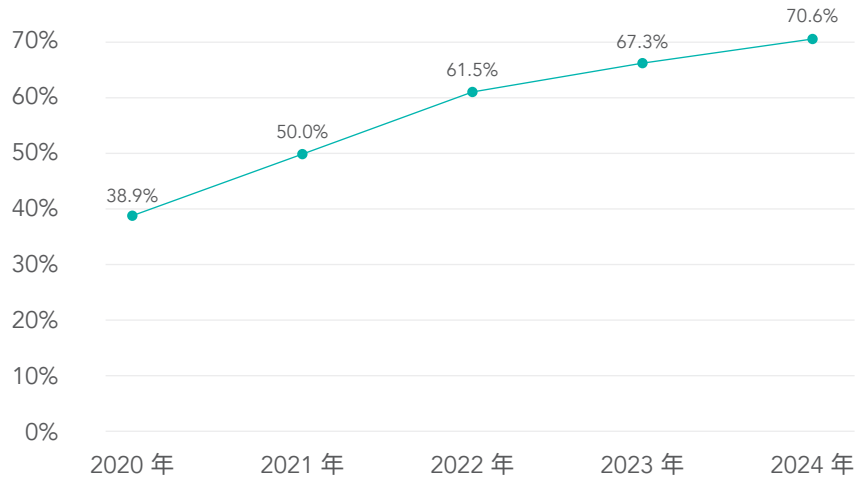


図 3:2020 年～2024 年の DMARC 採用率

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 の成長の理由となっています。DMARC は BIMI を設定する上で必須となるセキュリティ要件であり、両者は連動して E メールドメイン上の企業 ID の真正性を検証します。

レジストリロックの使用は着実に、しかし緩やかに増加

レジストリロックの採用率は、2020 年の 17% から 2024 年には 24% に上昇しました。また、エンタープライズクラスのレジストラを使用する企業は、レジストリロックを使用する頻度も高く、2024 年にはその割合は 45% となっています。サイバーセキュリティ強化への圧力が高まる中、より多くのレジストリが徹底したドメイン名トランザクションセキュリティを可能にすることで、人的エラーや サードパーティのリスクを軽減するためのドメイン拡張子のロックを提供しています。

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、そのドメインが企業運営やオンラインブランドにとって重要な業務を行っているかどうかを特定し 、ロックすべき重要なドメインを推奨します。

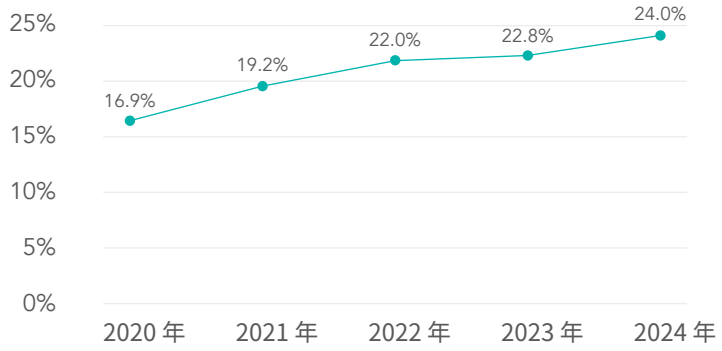


図 4：2020 年～2024 年のレジストリロック採用率

DNS 冗長化、DNSSEC、CAA レコードなどのセキュリティ対策は一貫性なし

DNSSEC を採用している企業の割合は依然として低 いものの、2020 年の 3% から2024 年には 9% と、過去 5 年間で 3 倍に増加しています。DNSSEC により、DNS クエリとレスポンスにおける認証とデータの整合性が可能となることで、サイバー犯罪者がインターネットトラフィックをフィッシングサイトなどの悪意のあるウェブサイトにリダイレクトする行為を防止することができます。

驚くべきことに、DNS 冗長化は今年も 1% 減少し、DNS の冗長化を優先する企業の割合は 2020 年よりも低下しました。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が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。

CAA レコードの利用は 2020 年の 4% から 2024 年には 10% に増加しています。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）に限定することができます。これにより、サイバー犯罪者が指定外の認証局を使って新しいデジタル証明書を取得する行為を防止することが可能になります。こうした行為が試みられてもリクエストは認められず、企業にアラートが送信されます。

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は レジストリロックを使用する頻度も高く、2024 年にはその割合は 45% となっています。

2024 年ドメインセキュリティ対策

地域別

EMEA では、2023 年から 2024 年の間に最大のドメインセキュリティ採用成長率が見られました。

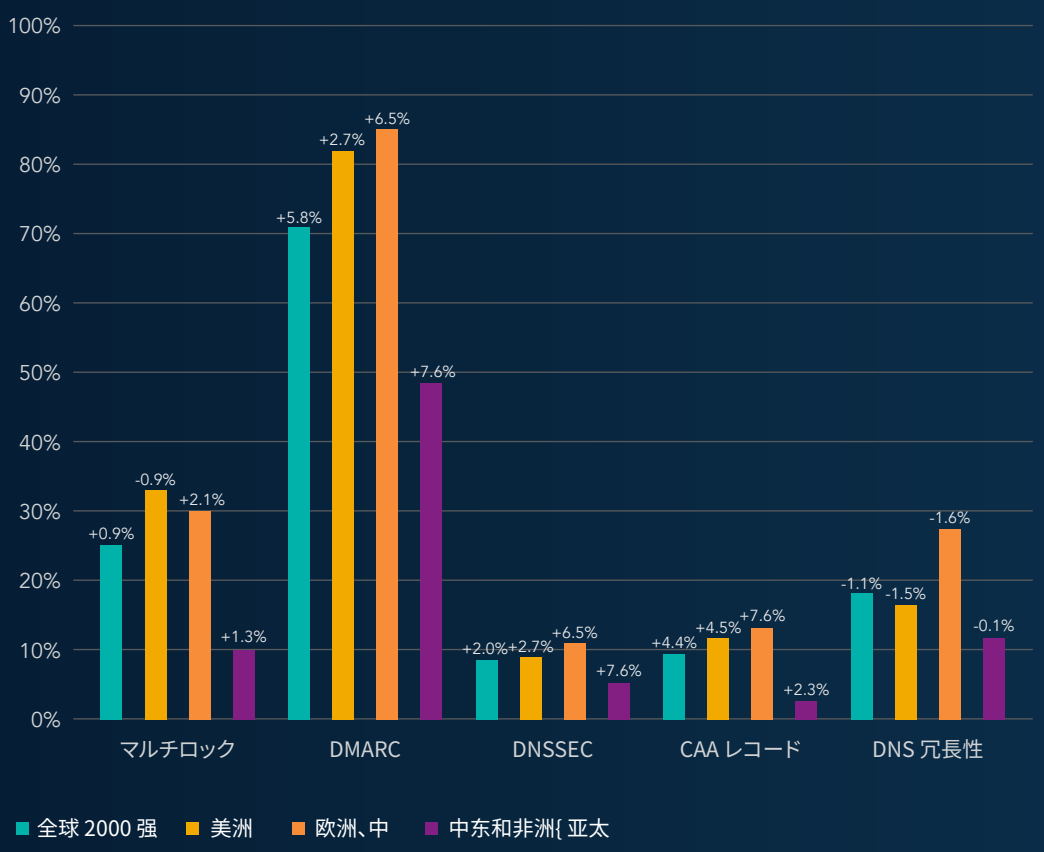


図 5：地域別ドメインセキュリティ採用率

業界別

2024年、医療業界は7つ順位を後退しています。

業界区分	2024 年ランキング	2023 年ランキング
テクノロジーハードウェア・機器	5	13 ↑
医療機器・サービス	12	5 ↓

「フォーブス・グローバル 2000」の 26 業界の中で、**医療機器・サービス**は 7 つ順位が下がって、これまで保持していた業界ランキングの上位 5 位から外れました。2023年の5位から2024年の12位へのランクダウンは、今年の病院や医療システムに対するサイバー攻撃の顕著な増加とは著しく対照的であり、特に医療部門がランサムウェア攻撃の最も頻繁な標的となっていることを考慮すると なおさらです。[1] 2024年はすでに、医療セクターで報告されているサイバーインシデントの数は 280 件に上っています。これは「2024 年における米国の全サイバーイベントの 24% にあたり、医療業界は他のあらゆる業界を圧倒」[2]しています。

テクノロジーハードウェア・機器は 8 位上昇して 5 位となりました。テクノロジー企業が上位 5 社にランクインするだけの体制を整えることは確かに有利となります。2020 年に発生したソーラーウィンズへの大規模なサプライチェーン攻撃以来、各社がセキュリティ対策を実施してきたことが、この成長率に関連している可能性があります。

↑ スコアが最も高い業界

- 小売
- テクノロジーハードウェアおよび機器
- 企業向け製品
- サービス

↓ 表現最差的行业

- 建設
- 食品・飲料・たばこ
- 食品市場
- 材料
- 石油およびガス

2024 年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、「グローバル 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。

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。ドメインセキュリティ用に設計されていない可能性のある、一般消費者グレードのレジストラに誤った信頼が寄せられており、企業の全体的なセキュリティ体制に影響が及ぶ可能性があります。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、詐欺防止、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としています。

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

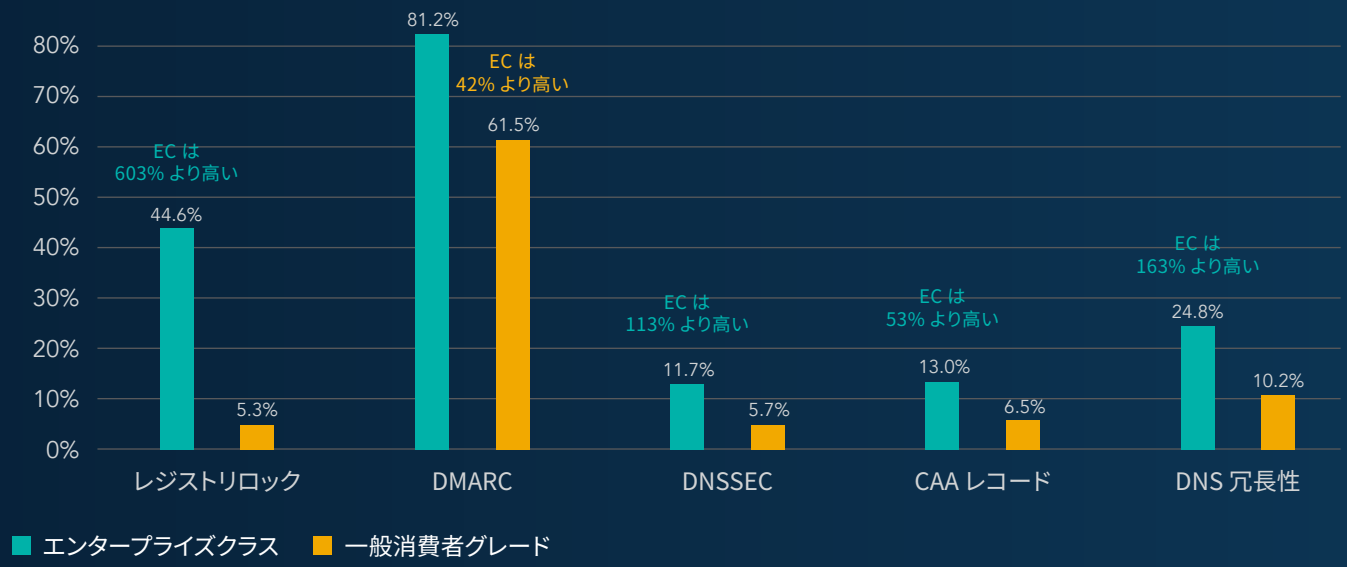


図 6：セキュリティ対策の熟成度：エンタープライズクラス（EC）と一般消費者グレード（CG）のレジストラ

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、ドメインセキュリティの脅威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（マルチロック）
- CAA レコード
- DNS 冗長化
- DNSSEC
- SPF (Sender Policy Framework)
- DKIM
- DMARC

ドメインセキュリティリスクレベル

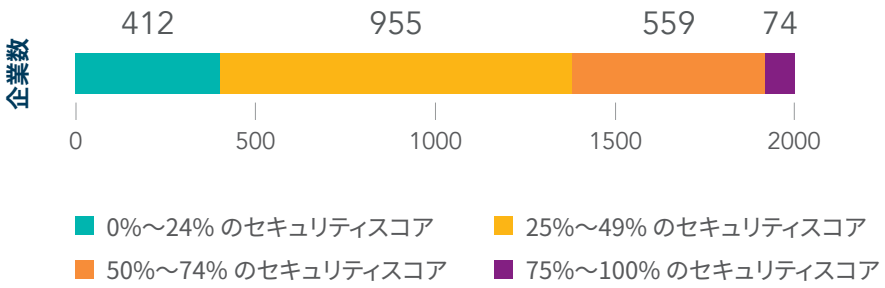


図 7:「グローバル 2000」企業のドメインセキュリティスコアおよび関連ドメインのセキュリティリスクレベル

「グローバル 2000」企業のうち68%は、推奨されるセキュリティ対策の半分以下しか実施していません。

スコアが最も高い企業

今年 100 %のスコアを獲得し、昨年も 100 %のスコアを獲得した企業は 1 社だけです。12 社が 8 点満点中 7 点のスコアを得ています。

スコアが最も低い企業

107 社のドメインセキュリティスコアがゼロとなっています。これらの企業は主にアジア太平洋地域の企業に見られ、スコアが 0 の企業の 87% を占めています。

「グローバル 2000」企業を標的とした不審なドメインまたは悪意のあるドメインによる攻撃

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。このようなサードパーティによるドメイン登録は、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するものです。これにより、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が発生する可能性があります。

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。

一般的なホモグリフは、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戦術

図 8：一般的なドメインなりすまし戦術

.COM ドメインにおける一般的なホモグリフ（あいまい一致）

フィッシングドメインでの頻繁な使用観察に基づき、当社の分析では、例えば「C0rnpanyNarne.com」を使用して「CompanyName.com」のように見せかけるなど、一般的なラテン文字の置き換えが含まれています

C0rnpanyNarne.com

よくあるアルファベットの置き換え

c → e　　0 → 0　　m → n　　l → I　　m → rn

g → q　　E → 3　　S → 5　　B → 8　　l → 1

図 9：.COM ドメインにおける一般的なホモグリフ（あいまい一致）

ホモグリフドメインの 80% 以上をサードパーティが所有

サードパーティ所有ドメインの中での割合：

42% 2024 年に MX レコードを所有している割合。2023 年の割合は 40%。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することが可能

サードパーティドメインの利用先

48% 広告やペイパークリックの広告を対象としている割合、ドメインパーキングに利用されている割合

33% 非アクティブなウェブサイトを所有している割合

2% ブランドの評判の失墜や顧客の信頼の喪失を招く恐れのあるコンテンツが含まれている割合

17% ブランド所有者に関連しないライブウェブサイトのアドレスに解決されるドメインの割合

サードパーティが所有する偽ドメインの登録に最も関連付けられるドメインレジストラ

- GoDaddy®
- Namecheap™
- Network Solutions

審なドメインおよび悪質なドメイン：標的

業界	全体の中で偽ドメインの脅威が占める割合（%）
銀行	19.9%
総合金融	7.2%
IT ソフトウェアおよびサービス	7.2%
建設	6.4%
保険	6.3%
石油およびガス	6.2%
公益事業	6.1%
資本財	5.5%
耐久消費財	5.3%
企業向け製品・サービス	5.0%
輸送	4.9%
材料	4.7%
小売	4.6%
テクノロジーハードウェアおよび機器	4.2%
医薬品およびバイオテクノロジー	3.5%
食品・飲料・たばこ	3.4%
医療機器・サービス	3.4%
通信サービス	3.0%
半導体	2.9%
化学	2.6%
航空宇宙および防衛産業	2.0%
ホテル・飲食・レジャー	1.7%
家庭用品・個人向け商品	1.7%
食品市場	1.5%
商社	1.2%
メディア	1.1%

ドメインセキュリティの洞察：2024 年のオリンピック期間中のドメイン急増から得られる教訓

2024 年 7 月にパリで開催されたオリンピック大会では、他の主要な世界的イベントと同様に、偽造品、偽チケット、詐欺的ストリーミングサイト、フィッシング攻撃など、世界規模の展開力を悪用しようとする詐欺師によるデジタル脅威が発生しました。こうしたデジタル脅威を軽減するには、よく似たドメイン名、失効ドメイン名、再登録ドメイン名、新規登録ドメイン名など、企業はセキュリティ体制やブランドのオンライン戦略において、ドメインエコシステムをグローバルに監視することを最優先する必要があります。企業は特に、現時点ではまだ武器化はされていないものの、攻撃インフラとなり得る兆候のある休眠ドメインに注意を払う必要があります。

ハイライト

今回の調査では、「オリンピック」という用語または「パリ 2024 大会」などの関連キーワードが含まれている独自のサードパーティドメイン名が 8,857 件特定されました。（図 10 参照）新規登録、失効、再登録を含め、2023 年 8 月 1 日から 2024 年 8 月 13 日の間に発生したドメイン活動を分析しました。図 10 に示されているように、オリンピックの開幕（7 月 26 日）と終了（8 月 13 日）に合わせて新規登録が急増しています。まだ登録されているドメインのうち、49% は休止状態で、アクティブなウェブサイトに接続されていませんでした。しかし、これらのドメインのうち、25% は MX レコードが設定されており、8% は SSL 証明書が適用されていました。

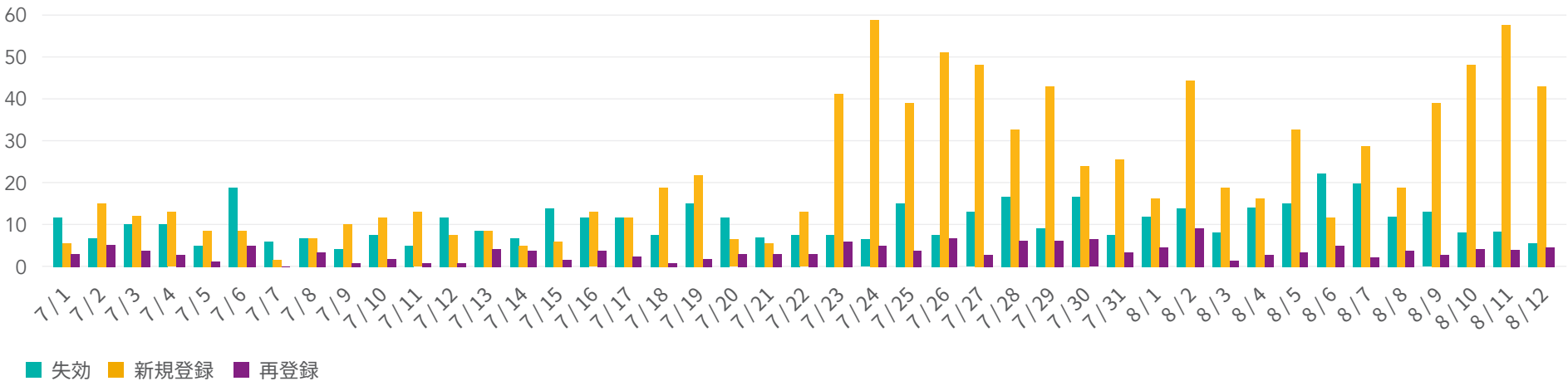


図 10：2024 年 7 月 1 日から 2024 年 8 月 1 日までのドメイン登録動向（60 日間）

主なポイント

休眠ドメインの悪用はいつでも起こり得るため、これらのドメインをリアルタイムで継続的に監視することは極めて重要です。悪意のあるドメイン名を追跡することで、企業は潜在的なリスク要因が顕在化する前に、より的確にこれを特定することができます。

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、企業の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、評判に対する大きな脅威となります。

対策を講じていない企業は、分野別トップレベルドメインや国別コードトップレベルドメインなど、グローバルドメインネームエコシステム全体で検索を行うべきです。CSC が提供する 3D Domain Security and Enforcement ソリューションなどの高度な監視サービスを活用することで、基本的な完全一致、ワイルドカード、タイプミスだけでなく、広範囲にわたるドメインバリエーションを検出することができます。さらに企業は、フィッシングサイト、マルウェアダウンローダー、タイポスクワッティングドメイン、偽の検索エンジン最適化サイト、ソーシャルメディアポータル、モバイルアプリストア、偽造品を販売するマーケットプレイスなど、さまざまな脅威に対して排除措置を実行できるプロバイダーと協力を図る必要があります。

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的な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 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、詐欺防止を重点領域とし、フォーブス誌の「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ちます。 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。CSC はまた、オンラインブランドの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プロテクションを提供し、特定のドメインを標的とするファイアウォール外のさまざまな脅威を多角的に把握します。 さらに、攻撃の初期段階でフィッシングに対処する不正防止サービスも提供しています。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。

お気軽にお問い合わせください

cscdbs.com/jp

[1]npr.org/sections/shots-health-news/2024/09/17/nx-s1-5111590/cyberattacks-ransomware-health-care-federal-response

[2]tebra.com/theintake/practice-operations/medical-news/the-major-cyberattacks-that-have-affected-healthcare-systems-in-2024

DBS12192024