ドメインセキュリティレポート 2026

はじめに

CSCは過去6年連続で、「フォーブス・グローバル2000」企業のセキュリティ体制を評価し、ドメインセキュリティの現状を調査してきました。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、「グローバル2000」企業と世界のユニコーン企業上位100社のドメインセキュリティ対策を比較しました。いくつかの類似点がある一方で、我々の重要な疑問のひとつに、これらの新しい企業（多くはテクノロジーやAI分野）が、より強力なドメインセキュリティ体制を採用しているかどうかという点がありました。報告書では、我々が発見したことが明らかにされています。

「グローバル2000」企業をはじめとする多国籍企業へのサイバー攻撃が増加する中、CSCは強固なドメインセキュリティに対する啓発を続けています。脅威は企業のITインフラのあらゆる分野から発生する可能性がありますが、ほとんどの攻撃はドメイン名を利用してシステムに侵入します。今や、強固なセキュリティ体制を確保することが、かつてないほど重要になっています。

主な調査結果の概要

ユニコーン企業は、DNSレコードを中心とした主要なドメインセキュリティ対策において強力な採用率を示しているものの、成熟するにつれて重大な見落としとなる可能性のある他の分野では遅れをとっています。

ドメインベースのメッセージ認証、レポーティング、コンフォーマンス（DMARC）、送信者ポリシーフレームワーク（SPF）、ドメインキー識別メール（DKIM）、DNSセキュリティ拡張（DNSSEC）、認証局認証（CAA）レコードなど、ドメイン名システム（DNS）レコードに依存するドメインセキュリティ対策については、ユニコーン企業の採用率は高く、メール認証プロトコルにSPFを使用している企業は100%に達しています。しかし、DNSの冗長化を採用しているのはわずか1%で、ユニコーン企業の90%近くがクラウド上の単一インフラを利用しています。

8種類のドメインセキュリティ対策のうち5つが「グローバル2000」企業よりもユニコーン企業で高い採用率

ユニコーン企業では、DMARC（96.0% 対79.8%）、DNSSEC（16.8% 対10.8%）、CAAレコード（33.0% 対11.4%）など、DNSレコードに関連するすべての指標において、「グローバル2000」企業よりも高い採用率を示しました。このことから、ユニコーン企業のドメイン名を管理するチームは、企業にとってコストがあまりかからないDNS内のセキュリティプロトコルに精通したIT専門家である可能性が高いと考えられます。これは、（技術）イノベーションを推進する企業として、より成熟した企業が見習うべき心強い傾向です。

「グローバル2000」企業で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と一般消費者グレード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採用に6倍以上の格差

レジストリロックは、レジストラアカウントが侵害された場合でも、ドメインとDNSに対する不正な変更を防止するため、DNSの乗っ取りに対する最も強力な防御策の1つです。このサービスをサポートするためにはリソースが必要なため、ほとんどの一般消費者グレードのレジストラはこのサービスを提供することができません。そして、このことは、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の採用率が6倍高く、強力なセキュリティ体制を示しているというデータからも明らかです。また、最近のレポート「SSL現状レポート」では、大企業の60%がセキュアソケットレイヤー（SSL）プロバイダーを3社以上利用しており、リスクが拡大していることが明らかになりました。この1年で企業にどれだけの損害をもたらしたかを私たちは目の当たりにしてきましたが、エンタープライズクラスのプロバイダーは、企業のデジタル環境をより適切に管理し、サプライチェーンにも同様の強固なセキュリティ体制を確保することができます。1

アジア太平洋（APAC）地域は2024年から2025年にかけて最大の伸びを示していますが、総採用率では欧州・中東・アフリカ（EMEA）地域と南北アメリカに依然として及ばず

アジア太平洋地域の企業では、この1年間で採用率が大幅に改善されましたが、実際の採用に関しては、アジア太平洋地域は他の地域よりも15%以上遅れています。

過去1年間で総合スコアが最も上昇したのは半導体業界と銀行業界

いずれも昨年より順位を5つずつ上げています。この2つの業界の急成長は、人工知能（AI）とフィンテックの台頭に後押しされたものであり、サイバーセキュリティに対する要求の厳しさも相まって、より優れたセキュリティ体制が認められたものと考えられます。

外部攻撃サーフェスはドメインエコシステムの拠点

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実行するために使用されています。

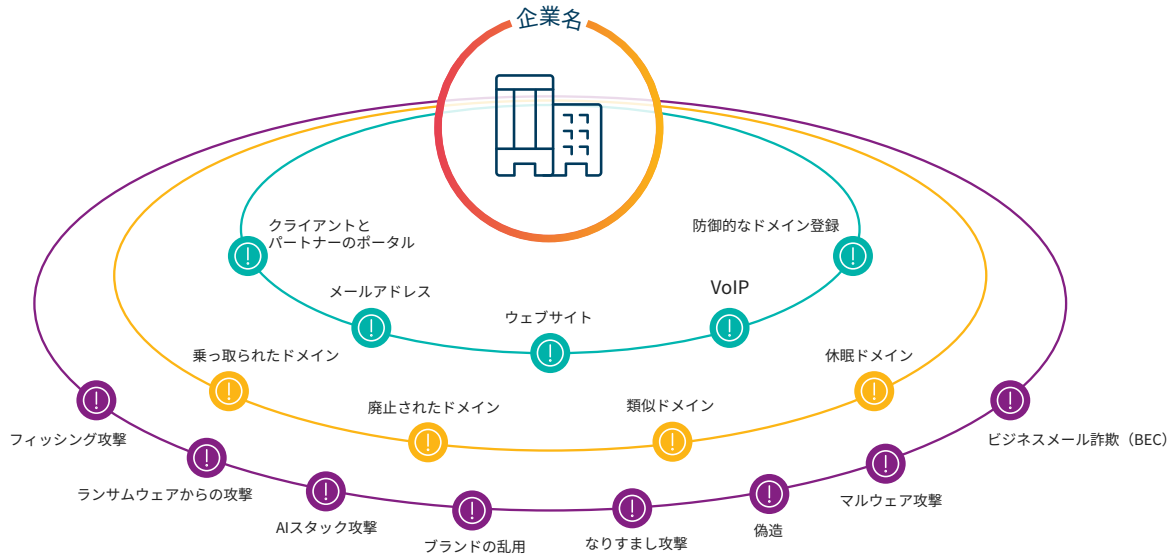


図1:ドメイン名エコシステムの全体図

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、サプライチェーン全体など、あらゆるものをインターネットに依存しています。インターネットは、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上で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規の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。この手法では、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、攻撃を開始するために登録されたドメインであることを示す兆候（例えば、通常であればレッドフラグとなるアクティブなMX（電子メール）レコードなど）がすぐに見られないため、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悪用して、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の濫用を仕掛けることにあります。

→ 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うした機会を捉え、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」企業のドメインセキュリティ対策の採用動向

この分析において、CSCは「グローバル2000」企業のドメインセキュリティ対策として、DMARC、DNSの冗長化、レジストリロック、CAAレコード、DNSSECの5つの主要な対策が採用されているかどうかを調べました。さらに、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いました。

ドメインセキュリティ対策の採用動向(2020年～2025年)

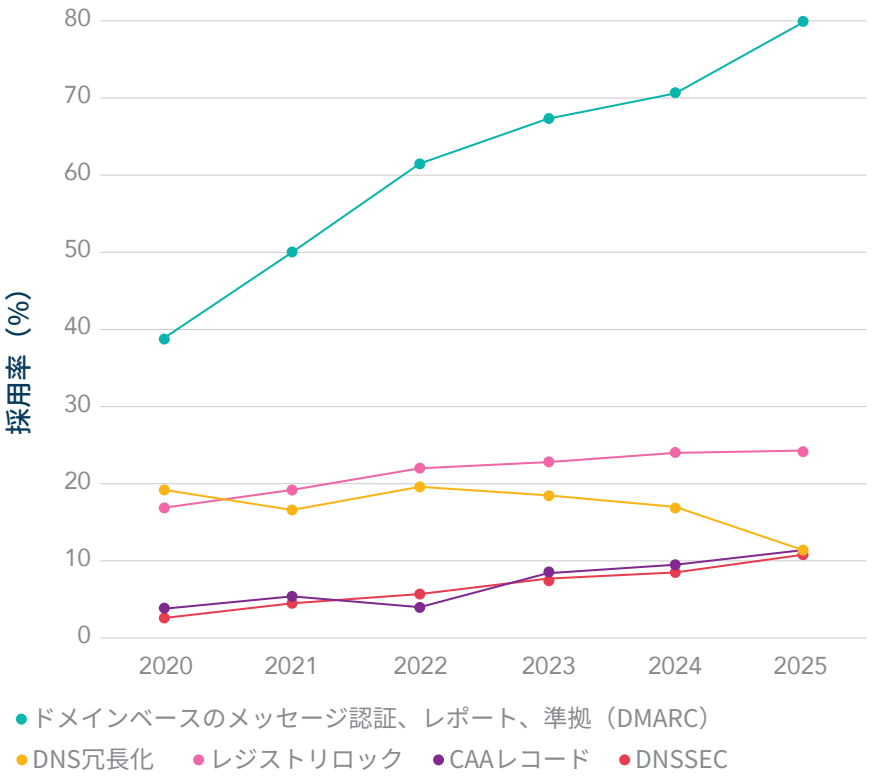


図2：「グローバル2000」企業の5主要ドメインセキュリティ対策の採用動向（2020年～2025年）

DMARCの成長が最速

DMARCの採用率が、2020年の39%から2025年には80%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（その件数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）また、2024年10月にNIS2が発効し、EUで活動する企業のサイバーセキュリティがより重視されるようになったことからも、DMARCの採用が進んでいます。まだ採用が遅れている残りの20%のうち、85%は全産業でアジア太平洋地域が占めており、これは地域別の採用に関する観測と一致しています。

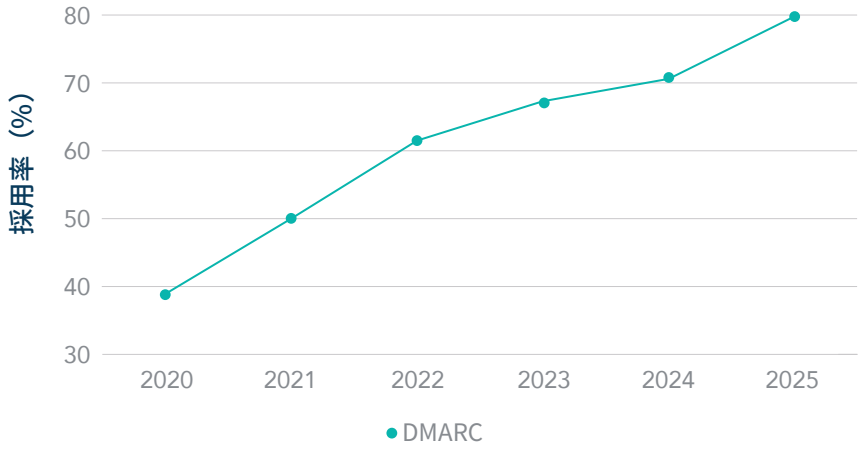


図3：2020年～2025年のDMARC普及率

NIS2とは何か？

「ネットワークおよび情報セキュリティ指令2」（NIS2）は、欧州連合（EU）が2022年12月14日に採択した新しいサイバーセキュリティ法（指令（EU）2022/2555）を指します。この指令は、EU加盟国全体でより高い共通レベルのサイバーセキュリティを確保するために、従来の指令よりも厳しい要件を定めています。特に、エネルギー、運輸、医療、銀行、金融、マーケティング・インフラ、デジタル・インフラ、および行政部門の組織を含む、重要事業体レジリエンス指令（CER）—指令（EU）2022/2557—に基づく重要事業体に対する義務を示しています。対象となる組織は、サイバーリスクを管理し、システムを保護し、インシデントに迅速に対応し、国のサイバーセキュリティ戦略を遵守するための具体的な措置を講じることが求められます。インシデントの報告が義務付けられている一方、脅威情報の共有が奨励されています。規制当局には、監査、コンプライアンスの実施、違反に対する罰金を組織に課す権限も与えられています。

このような国家レベルでのサイバーセキュリティの重視を受け、世界各国の政府も自国の重要産業に対して同様の指令を採択しています。例えばオーストラリアでは、「2023年～2030年オーストラリア・サイバーセキュリティ戦略」に、最低セキュリティ基準の義務化、報告義務の導入、リスク管理とデータセキュリティにおける規則と義務の明確化を盛り込んだ、新しいサイバーセキュリティ法（2024年）および重要インフラセキュリティ法（SOCI法）の改正が盛り込まれています。国際的に事業を展開する企業は、こうした国際的な基準の高まりに合わせてセキュリティ対策を実施する必要があります

DNS冗長化は減少

DNS冗長化の採用は昨年と比較して若干の減少を示しました。これはCSCの方法論が昨年と変更されたことも一因ですが、基礎的なデータでもわずかな減少が見られます。全体では前年比6%増となり、企業はDNSの冗長化を優先しています。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。また、多くの企業が、コスト削減、拡張性、データへのアクセス性などを求めて、クラウド上の単一インフラに移行しています。クラウド上にあることで、グローバルに分散されたシステムが提供される一方で、システムの一部がオフラインになった場合の潜在的なリスクは変わりません。DNSのリスクを真に軽減する唯一の方法は、冗長化のために2つの強固な独立したネットワーク（デュアルインフラ）を確立することです。

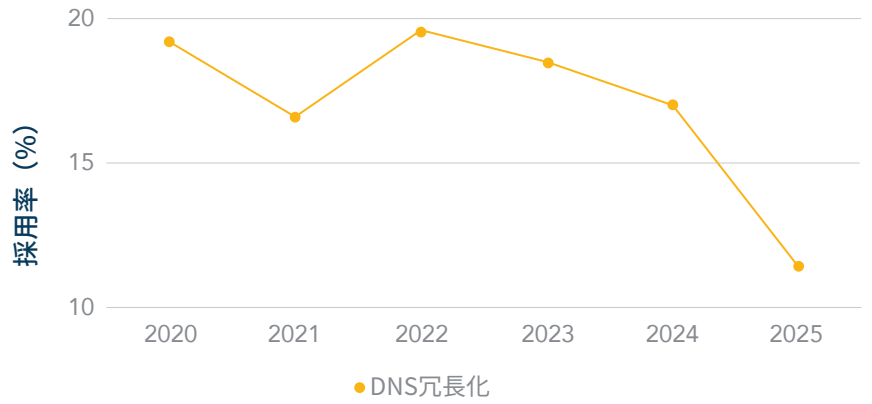


図4：2020年～2025年のDNS冗長化の採用率

DNSが今日のデジタルエコシステムにおける最大の単一障害点として浮上した理由をウェビナーでご覧ください。

レジストリロック、DNSSEC、CAAレコードなどのセキュリティ対策は、着実に、しかし緩やかに普及が進んでいます。

レジストリロックの採用率はわずかながら上昇し、2025年には24%になりました。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、2025年にはその割合は53%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。AIの台頭により、当社は今後も強力なドメインセキュリティ体制を信頼シグナルとして提唱しています。これは、アプリケーションプログラミングインターフェース（API）やプラグインを使用する企業のAIスタックがすべてドメインとDNSに依存して機能するため、特に重要です。

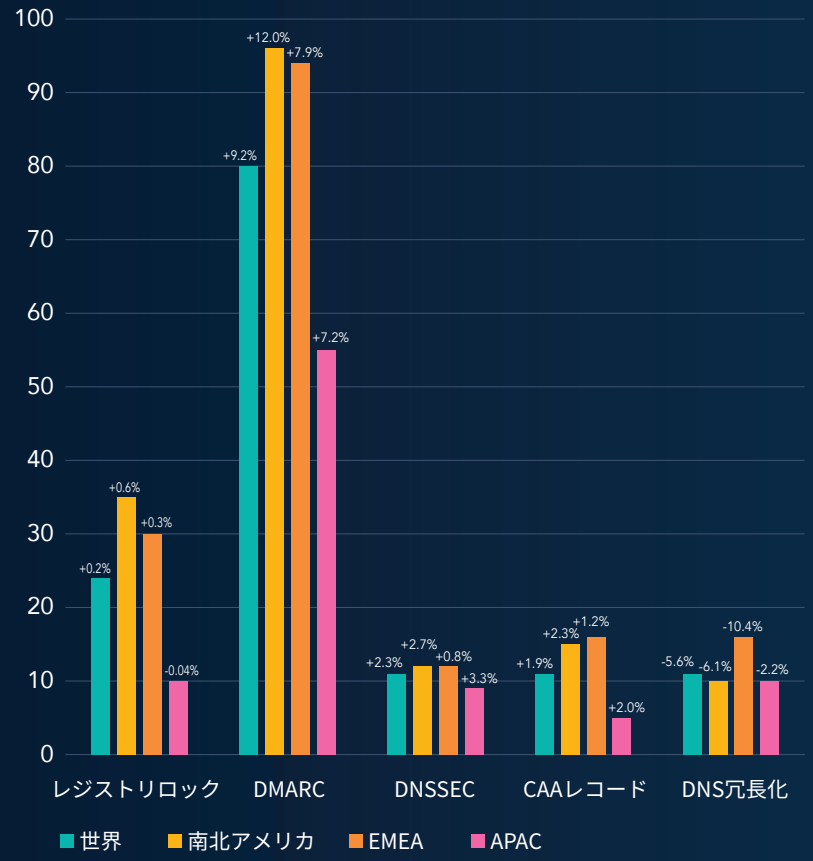
DNSSECを導入している企業の割合は、まだ低いものの、過去6年間で4倍に増加し、2025年には11%に達しています。DNSSECにより、DNSクエリとレスポンスにおける認証とデータの整合性が可能になることで、サイバー犯罪者がインターネットトラフィックをフィッシングサイトなどの悪意のあるウェブサイトにリダイレクトする行為を防止することができます。国によっては、DNSSECの採用率が67%を超えるところもあります。しかし、大規模な組織ではまだ低水準にとどまっています。これは、より複雑な組織構造でキーの更新を維持する必要があることが原因の一部ですが、すべての重要ドメインが採用すべきセキュリティ対策であることに変わりはありません。

最後に、CAAレコードの採用率は再び上昇し、2025年には11%になりました。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。なぜなら、リクエストは認められず、企業にアラートが送信されるからです。CAAレコードのもうひとつの利点は、企業がコンプライアンスを徹底することで、従業員が許可されたプロバイダーのみを利用するようにできることです。当社の最新レポート「SSL現状レポート」では、大企業の60%以上が3社以上のプロバイダを利用しており、中には13社のプロバイダを利用している企業もありました。このレポートはまた、詐欺サイトで最も多く利用されているプロバイダが、最も多く利用されているプロバイダでもあることを強調しています。特にAIスタックの自律化が進む中、SSL管理のさらなる精査が必要です。

ドメインセキュリティ対策

ー地域別

アジア太平洋地域は、2024年から2025年にかけてドメインセキュリティの採用が最も伸びていますが、総採用率では欧州・中東・アフリカ地域と南北アメリカに遅れをとっています。



対前年増減率（%）

図5：地域別ドメインセキュリティ採用率

ー業界別

ITソフトウェアとサービス業界は、2025年においても引き続きトップを維持しています。

業界区分	2025年ランク	2024年ランク
半導体	6	11
銀行	11	16
テクノロジーハードウェアおよび機器	13	5
航空宇宙および防衛産業	16	8

最も高いスコアを示しているのは、ITソフトウェアやサービス、メディアなど、事業運営をインターネットに大きく依存している業界です。また、銀行や半導体も昨年よりさらにスコアを上げています。この2つの業界の急成長は、人工知能（AI）とフィンテックの台頭に後押しされたものであり、サイバーセキュリティに対する要求の厳しさも相まって、より優れたセキュリティ体制が認められたものと考えられます。スコアが低迷している業界としては、建設業、鉱業、公益事業などが挙げられます。興味深いのは、低スコアの業界の多くが、特にNIS2指令では重要産業にも分類されていることです。これは、特にこうした業界への攻撃が増加していることから、来年以降、これらの業界がドメインセキュリティにより真剣に取り組むようになることを意味しているのかもしれません。

↑ 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
- 小売
- 企業向け製品・サービス
- 通信サービス

↓ スコアが最も低い業界

- 建設
- 材料
- 食品市場
- 公益事業
- 食品・飲料・たばこ

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。エンタープライズクラスのレジストラの使用により、ドメインの乗っ取り、ダングリングDNS、およびドメインのなりすましをいかに軽減できるかについて詳しくは、当社の「ドメインセキュリティチェックリスト」をダウンロードしてご覧ください。

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。多くはドメインセキュリティサービスを提供していないため、採用率の低下にもつながっています。

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

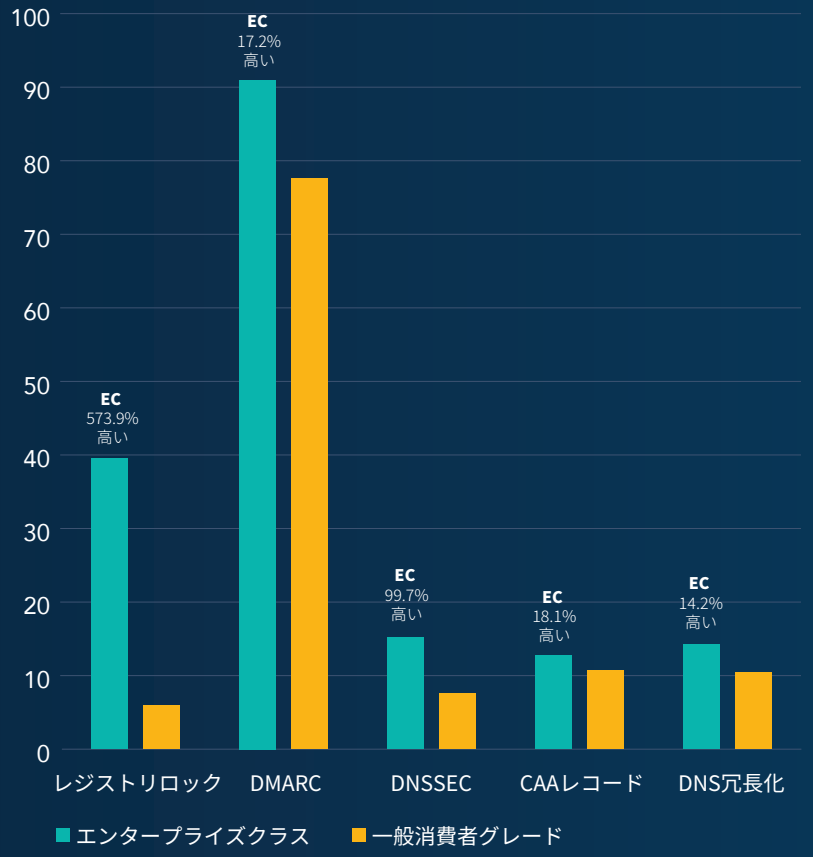


図6：セキュリティ対策の熟成度：エンタープライズクラス（EC）と一般消費者グレード（CG）のレジストラ

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、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ドメインレジストラ
- 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)
- ドメインキー識別メール（DKIM）
- DMARC

ドメインセキュリティリスクレベル

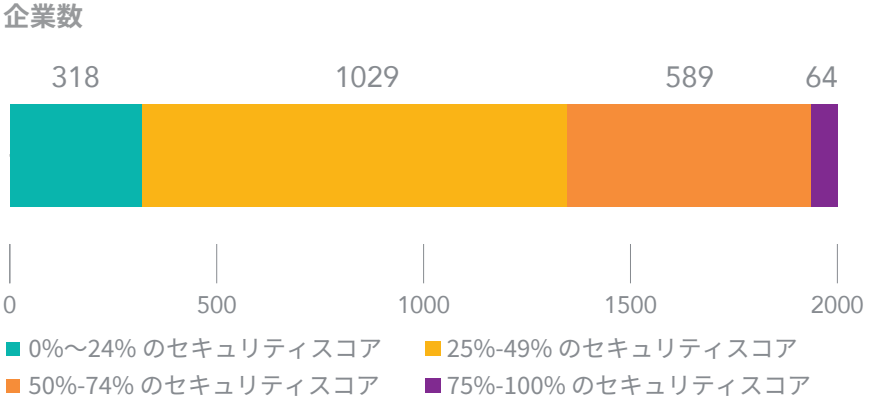


図7：「グローバル2000」企業のドメインセキュリティスコアおよび関連ドメインのセキュリティリスクレベル

「グローバル2000」企業のうち67%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ない

↑ スコアが最も高い企業

100%の企業は、昨年と同じく1社に留まりました。8点満点中7点を獲得した企業はわずか8社で、これは昨年より3分の1減少しています。

↓ スコアが最も低い企業

ドメインセキュリティのスコアがゼロだった企業は87社で、昨年の107社から改善されました。これらの企業は主にアジア太平洋地域の企業であり、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の手法

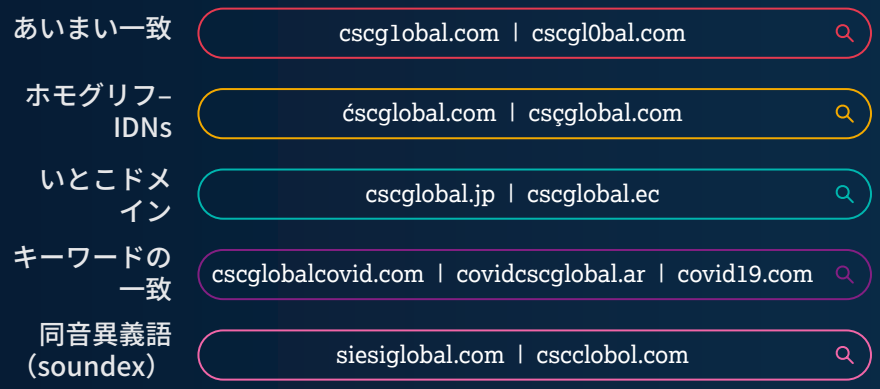
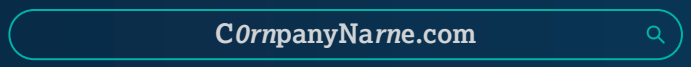


図8：一般的なドメインなりすまし戦術

.COMドメインにおける一般的な紛らわしい文字列（あいまい一致）

当社の分析では、フィッシング・ドメインでの頻繁な使用観察に基づき、例えば、C0rnpanyNarne.comを使用してCompanyName.comのように見せるなど、一般的なラテン文字の置き換えも対象としました。



よくあるアルファベット置き換え

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紛らわしい文字列(あいまい一致)

ホモグリフドメインの80%以上は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：

40% 2025年にMXレコードを保有している割合（2024年は42%）
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。
これは、DMARCレコードの追加が増えている主な理由です。

サードパーティドメインの利用先

40% 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

39% 非アクティブなウェブサイトを所有している割合

32% アクティブなメールレコードを持つ非アクティブドメインの割合
これは、ライブコンテンツに解決されないドメインでも、メールの送受信に使用できることを意味します。

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

19% 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

企業が注意すべき領域の1つとして休眠ドメインの利用が挙げられます。これは、サードパーティが大量登録を行い、その名前を長期にわたって休眠させておくというものです。結果からわかるように、サードパーティドメインの32%は非アクティブですが、それらは簡単にアクティブ化できるMXレコードを含んでいます。

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

不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	16.3%
ITソフトウェアおよびサービス	6.6%
総合金融	5.8%
公益事業	5.4%
保険	5.4%
建設	5.2%
石油およびガス	5.1%
企業向け製品・サービス	4.3%
資本財	4.3%
輸送	4.3%
耐久消費財	4.0%
小売	3.6%
テクノロジーハードウェアおよび機器	3.6%
材料	3.5%
食品・飲料・たばこ	2.8%
通信サービス	2.7%
医薬品およびバイオテクノロジー	2.4%
医療機器・サービス	2.4%
半導体	2.3%
航空宇宙および防衛産業	1.9%
商社	1.7%
化学	1.7%
食品市場	1.5%
ホテル・飲食・レジャー	1.3%
家庭用品・個人向け商品	1.0%
メディア	0.9%

ドメインセキュリティに関する洞察：ユニコーン企業は有望なドメインセキュリティ支持者か？

CSCは今年、「グローバル2000」企業（その多くは老舗産業）とユニコーン企業上位100社を比較することにしました。ユニコーン企業上位100社の大半はIT企業で、その多くがAI産業です。単純化するために、これらの企業について「グローバル2000」企業と同じドメインセキュリティ特性を調べました。この分析の主な目的は、小規模な新興企業が大規模な既存企業よりもドメインセキュリティのリスクに敏感で、対策を実施する能力を持っているかどうかを確認することでした。また、AI業界で事業展開している多くの　ユニコーン企業は、ドメインやDNSといった重要なインフラ周りのセキュリティプロトコルが必要であることをよく理解しており、ある領域では高い採用率を示していますが、他の領域では不足しています。さらに、これらの企業の多くが構築しているAIスタックは、それらを使用する企業のサプライチェーンにおいて、より広範なリスクへとつながります。

ユニコーン企業とは？

ユニコーン企業とは、評価額が10億ドルを超える未上場企業を指します。こうした企業はたいてい新興企業や比較的新しい企業で、その業界では革新的な存在です。

注目ポイント

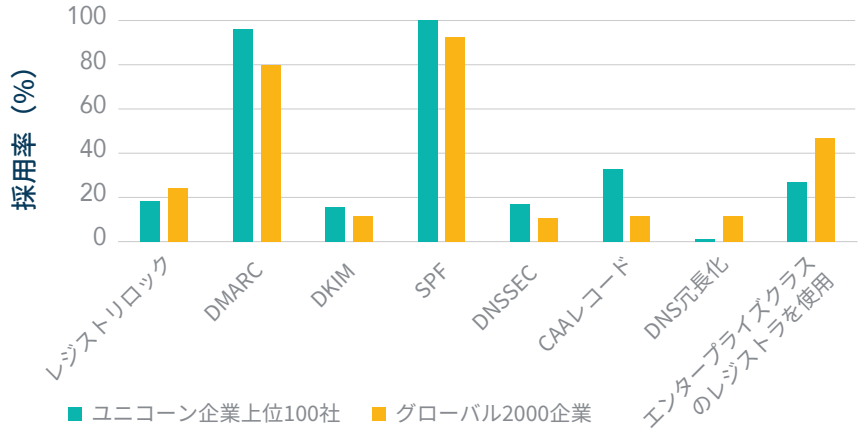


図10：ドメインセキュリティの採用率―「ユニコーン企業上位100社」対「グローバル2000」企業

8つのドメインセキュリティの属性で「グローバル2000」企業と比較すると、ユニコーン企業は5つのカテゴリーで高いスコアを示しています。特に、SPF、DKIM、DMARC、DNSSEC、CAAレコードの採用が進んでおり、電子メールのセキュリティが強化されています。これらに共通するのは、DNSレコードで管理されているという点です。このことから、ユニコーン企業のドメイン名を管理するチームは、企業にとってコストがあまりかからないDNS内のセキュリティプロトコルに精通したIT専門家である可能性が高いと考えられます。

「グローバル2000」企業がより高いセキュリティスタンスを持つという状況は、より多くの企業がエンタープライズクラスのレジストラを利用していることがまず第一の原因です。ここで重要な点は何かというと、エンタープライズクラスのレジストラは、ソーシャルエンジニアリングに対するスタッフへのトレーニングや、二要素認証といった強力なセキュリティ対策を講じていることです。一般消費者グレードのレジストラを使用している企業では、アカウントがハッキングされ、正規のドメイン名にサブドメインが設定される「ドメインのドッペルゲンガー化」などの行為が確認されています。

もうひとつの違いは、レジストリロックの利用率が低かったことです。これは、一般消費者グレードのレジストラの多くがこのサービスを提供していないという事実に起因しています。エンタープライズクラスのレジストラを使用している「グローバル2000」企業が、レジストリロックを採用する可能性はより大きいと言えます。

ユニコーン企業はまだ市場の成長に焦点を当てた初期段階にあるため、レジストラの選択はビジネスの優先事項の中では低い可能性があるほか、レジストラ間のさまざまな違いやそれがセキュリティ体制にどのように影響するかについての知識が不足している可能性もあります。レジストラのタイプは、レジストリロックの採用とセキュリティに直接影響します。なぜなら、このようなロック機能は一般消費者グレードのレジストラではサポートされていないためです。したがって、ユニコーン企業は、追加の防御層がないためにレジストラがより容易に侵害されると、DNSの乗っ取り、ドメインの乗っ取り、電子メールのなりすましなどの攻撃に対して脆弱になります。優れたDNSの基礎知識を備えた強力なITチームがあっても、ユニコーン企業はより大規模で複雑なドメインポートフォリオで事業を拡大する中で、サードパーティのドメインレジストラにドメインセキュリティを任せたままでは、大きなリスクをもたらす可能性があります。インシデントやダウンタイムが発生すると、オンラインで事業を展開するこれらの企業の大半に直接影響が及ぶからです。

AIとテクノロジーが優位

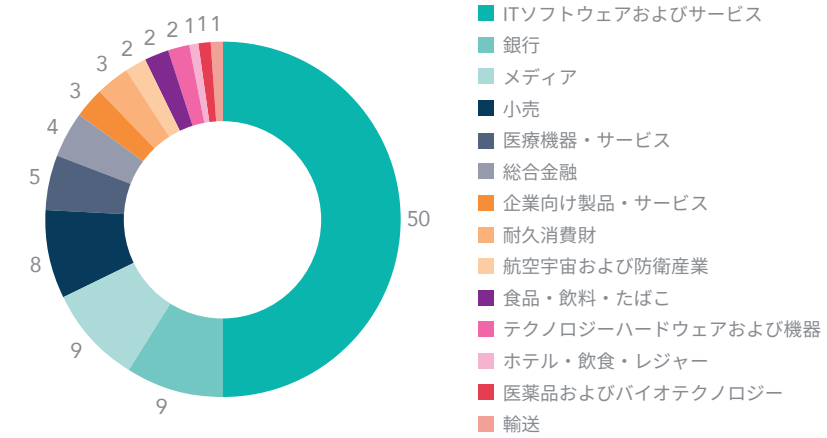


図11：ユニコーン企業上位100社に占める主な業界

ユニコーン企業上位100社の半数がITサービス企業で、次いで銀行が2位となっています。ITサービス企業の多くはAI企業で、銀行企業の多くはフィンテック新興企業となっており、いずれもインターネットに依存したビジネスを展開しています。

より安全なのは誰か？

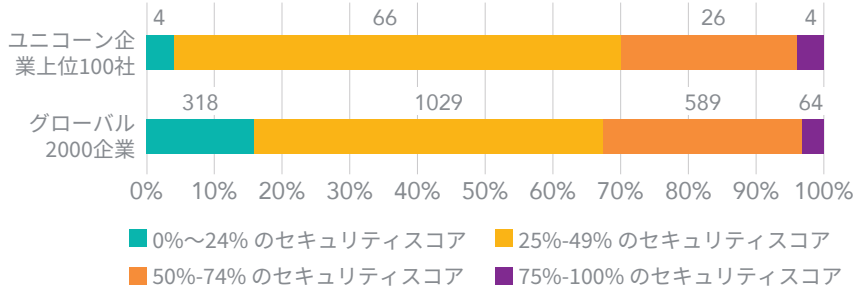


図12：ドメインセキュリティレベル―「ユニコーン企業上位100社」対「グローバル2000」企業

「グローバル2000」企業のドメインリスクスコアとユニコーン企業のドメインリスクスコアを比較しても、包括的な違いは見られません。「グローバル2000」企業の15%に比べ、ロースコアの範囲にいるユニコーン企業は4%と少ないことが明らかです。しかし、ミドルレンジに位置するユニコーン企業が著しく多く、これはメールのセキュリティなどの特定の要素には本格的に取り組んでいることがわかりますが、レジストリロックやDNS冗長性といったより高度なセキュリティプロトコルについては遅れを取っています。

結論

企業のドメインセキュリティは徐々に向上していますが、世界的な大企業の中でもまだまだ改善が必要です。特に、多国籍企業に対するサイバー攻撃が増加の一途をたどっていることから、NIS2のような法律による政府の介入は、このような変化をより迅速に推進することに重点を置くようになるものと予想されます。

ユニコーン企業は、DNSセキュリティに関連するドメインセキュリティプロトコルを迅速に採用していますが、これは多くの場合、グローバルに分散した企業のような複雑さを伴うことなく、迅速な意思決定を行うことができる、より小規模で機敏なIT部門によって支えられています。とはいえ、DNSの冗長化、レジストリロック、エンタープライズクラスのレジストラなどの分野では後れを取りがちです。しかし企業が成熟し、使用するベンダーがより洗練されるにつれて、この傾向は変わる可能性もあります。将来的には、ユニコーン企業は、自社のドメインセキュリティとサプライチェーンのドメインセキュリティの両方、およびユニコーン企業が属するサプライチェーンのドメインセキュリティを確実に強化することが必要になるでしょう。多くのユニコーン企業が事業を展開しているAI業界の重要性が高まっているにもかかわらず、重大なインシデントや政府による介入がなければ、喫緊の対応を促すのは難しいかもしれません。これは、セキュリティが事業推進の最重要事項であることを示しています。

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。

企業がドメイン名のセキュリティに真剣に取り組まなければ、サードパーティに悪用される恐れがあります。地政学的なシステムが刻々と変化し、犯罪者がより巧妙になり、悪意のあるサイバーキャンペーンにAIが導入される中、我々は一丸となって、標的になりにくいようにする必要があります。

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DomainSec℠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。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]cnbc.com/2025/09/21/what-we-know-about-the-cyberattack-that-hit-major-european-airports.html

DBS14112025