CSC

2022年版
ドメイン セキュリティ レポート

主な調査結果の概要 — 2022年の新機能は？

CSCは、過去3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報告してきました。今年は、一部の企業の安全性がより向上していますが、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。当社で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ベストプラクティスを共有して、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。

約3/4

グローバル2000企業の約3/4が、セキュリティの脅威にさらされる危険性が非常に高い

グローバル2000企業の4分の3近くが、全領域のセキュリティ対策の半分以下しか実施していない。CSCは、8つの主要なセキュリティ対策に着目し、各企業の平均スコアを算出しました。スコアが高いほど、セキュリティ体制が強固であることを示しています。

45%

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

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ー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5%のみです。ロックが掛かっていないドメインは、ソーシャルエンジニアリングの手口に対して脆弱であり、不正なDNS改ざんやドメインハイジャックにつながる恐れがあります。

75%

「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た割合

「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紛らわしい文字列 (フェイク) ドメインの75%のうち、2021年の77%と比較して、2022年には82%のWHOISまたは所有権の詳細がマスクされており、より多くの企業がWHOISプライバシー保護を使用していることを示しています。

<5%

他のプロアクティブなドメインセキュリティ対策の実装における成長率

企業は、手頃な価格のサイバー保険料金の資格を得るのに苦労しており、ドメインセキュリティは、他のサイバー費用と比較して、比較的低コストで修正できる分野の1つです。ドメインセキュリティを整備しないことは、フィッシング攻撃やランサムウェア攻撃、およびその他の多くのサイバー脅威につながる可能性があるため、当社は、レジストリロック、ドメインネームシステム (DNS) の冗長性、DNSセキュリティ拡張 (DNSSEC)、および認証局承認 (CAA) レコードなどのセキュリティ対策のより高度な実装を期待していました。

23%

最も高い成長率を示したDMARCの成長

Anti-Phishing Working Group (APWG) の最新の数字によると、フィッシング攻撃の数はかつてないほど増加しており、2020年の10倍になっています。ドメインベースのメッセージ認証、レポート、および準拠(DMARC)の増加につながったことは驚くことではありません。DMARCは、企業のEメールドメインがスプーフィング、フィッシング詐欺、およびその他のサイバー犯罪に使用されるのを防ぐために設計されたEメール検証システムです。

ゼロトラストセキュリティモデルが最重要の防御セキュリティ戦略になるにつれて、2022年は、ドメインセキュリティ採用の重要性が示されました。

ゼロトラストモデルは、ビジネスシステム、アプリケーション、およびデバイスを超えて拡張する必要があり、図1に示したように、攻撃に対する実際の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。次の2つのドメインセキュリティの脅威を使用することで、以下に示すすべての攻撃が可能になります。

図1

グローバル企業は、ウェブサイトからEメール、認証、VoIPなど、あらゆる作業をインターネットに依存しています。しかしそれは、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。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、フィッシング攻撃を含む新たな展開について学んでおり、それらが必要とする対象範囲とそれらを阻止する方法に関して、さらに複雑なレイヤーを追加しています。

ドメインセキュリティの定義

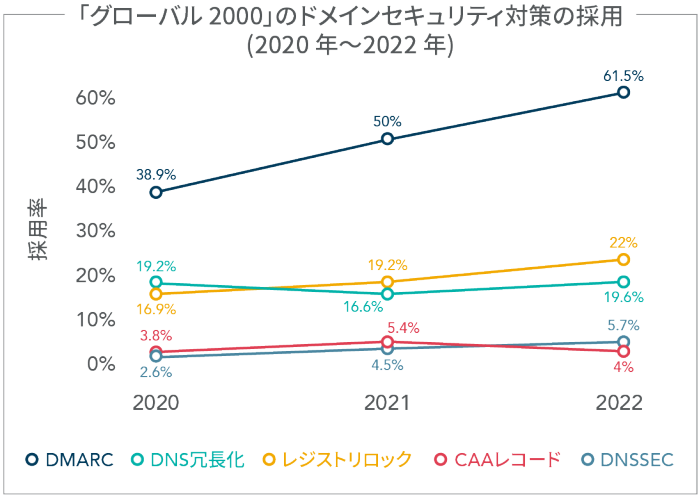
CSCは、階層化アプローチでドメインセキュリティを管理します。まず、買収などによって複数のブランドで構成されるドメインポートフォリオ、およびオンラインDNSフットプリントを確保することで、ブランドのオンライン事業を確保する必要があります。第2に、オンラインブランドを標的とする脅威ベクトルを監視し、分析し、権利を行使します。最後に、これらの他の2つのデータセットをファイヤーウォールの背後にある内部データセットで補完し、ブランドのセキュリティ体制を完全かつ包括的に把握します。

このレポートは、「グローバル 2000」企業のセキュリティ体制に焦点を当てており、リストはForbesによって毎年更新されます (つまり、毎年新しい企業がリストに掲載され、以前リストに掲載された企業でも上位2000にランクされない場合があります)。このレポートで共有されている洞察は、機械学習、AI、およびディープサーチテクノロジーを活用した独自のデータレイクを介して管理・公開されているデータセットのみに基づいています。

結果と分析

CSCは、「グローバル 2000」の全企業に対して以下の各ドメインセキュリティ対策導入の状況を分析し、産業および地域ごとの詳細も深く掘り下げて調査しています。

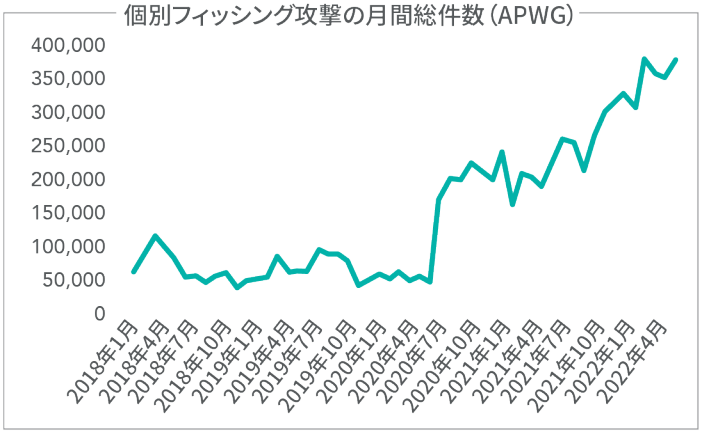
ドメインセキュリティ対策の採用動向（2020年～2022年）



DMARCの利用は2年間でほぼ倍増

DMARCの使用が2020年の39%から2022年の62%へ急速に増加したことは、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加を含む) を考えると驚くことではありません。

APWGの最新の数字によると、フィッシング攻撃の数はかつてないほど増加しており、2022年第1四半期には、特定された固有のフィッシング攻撃の四半期合計が初めて100万件を超え、毎月600を超える様々なブランドが攻撃されています。



また、検証済みマーク証明書(VMC)がセキュアソケットレイヤー(SSL)証明書を確認するためにDMARCの設定を必要としていることも、DMARCの成長の理由となっています。さらにAppleは、メッセージ識別用のブランド指標 (BIMI) を9月に発表し、iOS16およびmacOS用のEメールクライアントが幅広い業界の取り組みをサポートし、ブランドスプーフィングやなりすましに対応すると述べました。BIMIをサポートする送信者は、Eメール認証の厳しい基準を満たす必要があり、DMARC セキュリティ基準の使用が含まれます。

正規の送信元からなりすましEメールが送られたように見せかけることは非常に簡単です。DMARCを使用してEメールチャネルを認証すると、Eメールのスプーフィングや潜在的なフィッシングの発生を最小限に抑えることができますが、このように制御してもDMARC拒否ポリシーを採用しない場合はフィッシングのリスクが生じるため、本ポリシー実装の必要性が理解されています。

レジストリロック、DNS冗長性、DNSSEC、CAAレコードなどのセキュリティ対策は一貫した成長を遂げていますが、そのスピードは早くありません

レジストリロックを有効にしている企業率は、2020年の17%から2021 年には19%、そして2022年には22%に増加しました。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ーによるリスクを低減することができます。これは、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、世界中すべてのレジストリがロックサービスを提供している訳ではなく、ロックできないドメインもあります。

DNS冗長性とDNSSECを導入している企業は、過去3年間でわずかに増加しています。DNSはあらゆる組織のコアインフラストラクチャの重要なコンポーネントとなるため、より多くの政府機関がDNSの回復力を求めています。組織のステップアップを求めるプレッシャーの高まりと合わせて採用が求められますが、採用率の上昇はまだ見られず、これは企業がコストとリソース割り当ての増加を計画する必要があるためと思われます。

最後に、CAAレコードの使用は2020年から2021年にかけてわずかに増加しましたが、2022年には再びわずか減少しました。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) に限定できます。これによってサイバー犯罪者が指定されていない認証局からの新しい証明書の取得することを防ぎます。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SSLに複数のプロバイダを使用する場合は特に要件のナビゲートが難しいことが多く、多くの企業はまだこのセキュリティ制御を十分に使用していません。

2022年のレジストラタイプ別ドメインセキュリティ対策

本レポートでは、「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に関して、ドメインセキュリティの採用傾向を分析しました。

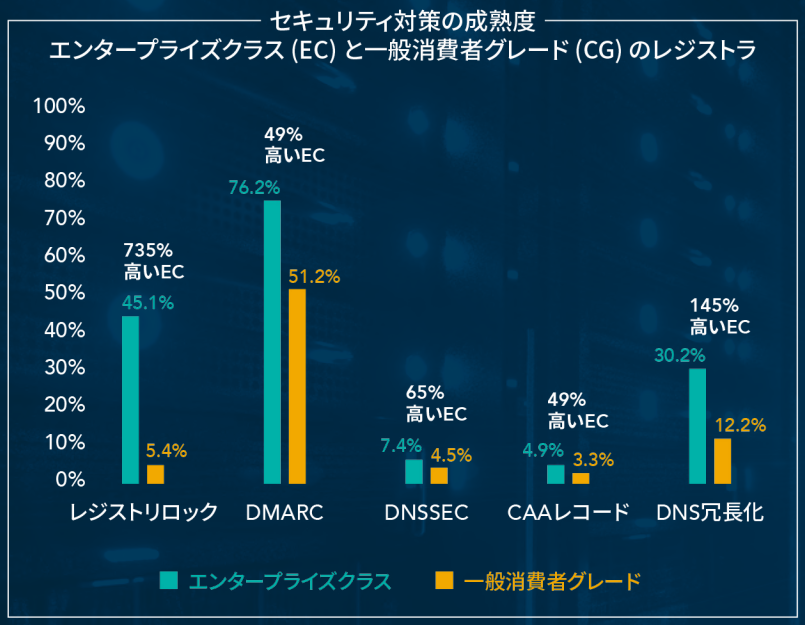
一般消費者グレードのレジストラ:

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、フラウド防止、データガバナンス、サイバーセキュリティに関連する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る可能性のあるドメインセキュリティ用に設計されていない場合があり、誤った信頼が置かれている可能性があります。一般消費者グレードのレジストラのほとんどはこれら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です。

2021年の後半、SecurityScorecardは一般消費者グレードのレジストラおよびエンタープライズクラスのレジストラを使用する企業のサイバー率を調査しました。その調査結果は、エンタープライズクラスのドメインレジストラによってドメイン管理している企業は、全体的なサイバーセキュリティの評価が0.5から1グレード高いことを示しています。

詳細を見る:

- ドメインセキュリティはレジストラ選びから始まる
- サイバーセキュリティは、利用している最も脆弱なベンダーと同レベルである
- ベンダーの選択には ドメインレジストラのエコシステムが重要である

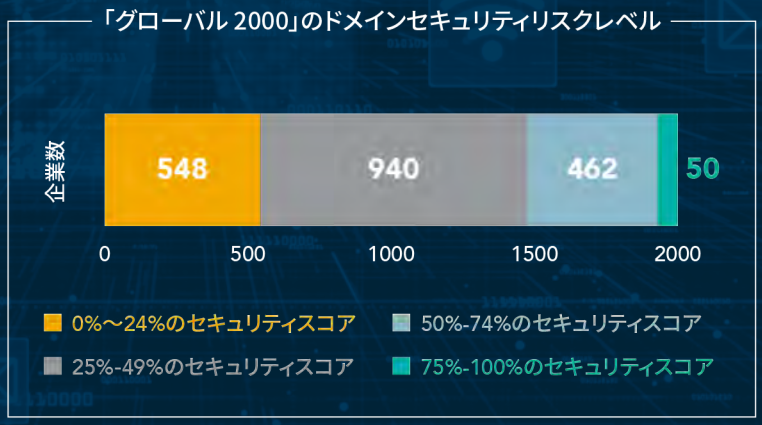
全体的なドメインセキュリティ体制

CSCは企業の**ドメインセキュリティリスクレベル**に従ってグループ化した 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得ました。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、企業がドメインセキュリティの脅威のリスクにさらされていないということです。

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
- DKIM
- DMARC

ほぼ3/4の企業が、すべてのドメインセキュリティ対策の半分未満しか実装していません



高業績を上げている企業のトップ5

- ITソフトウェアおよびサービス
- 企業向け製品・サービス提供
- ホテル・飲食・レジャー
- メディア
- 航空宇宙および防衛

スコアが最も良かった企業

6 最も多くのドメインセキュリティ対策を採用し、最高のセキュリティスコアを獲得した企業数。

2/3 これらの企業のうちのアメリカ企業の割合。

スコアがふるわない5つの業界

- 耐久消費財
- 食品市場
- 建設
- 商社
- マテリアル

スコアが最下位の企業

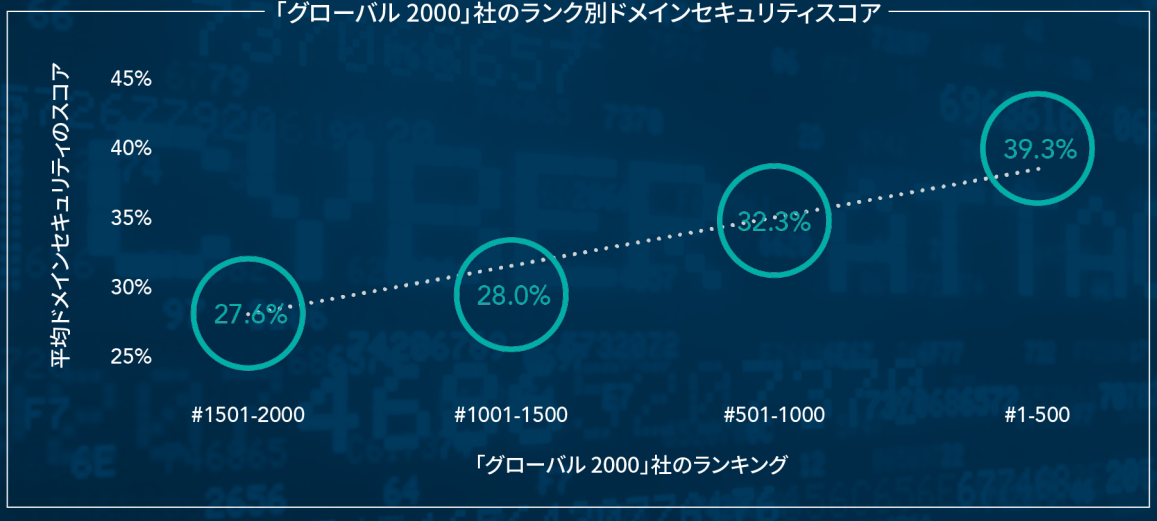
137社 ドメインセキュリティスコアが0でした。

これらの企業は主にAPAC地域の企業であり、スコアがゼロの企業の **82%**を占めています。

食品市場、マテリアル、建設などの業績の最も低い業界は、ドメインポートフォリオのセキュリティ対策が欠如しているため、サイバー攻撃のリスクが最も高くなります。サプライチェーンも、これら3つの業界がすでに取り組んでいる無数のマテリアル、労働力、および流通と同様の課題を抱え、さらに多くの問題を引き起こしています。耐久消費財も、自動車会社を含む下位5業種に入っています。モノのインターネット(IoT) が新車においてよりパーソナライズされた機能の大きな部分を占めるようになり、これらの企業がより強力なサイバーセキュリティ体制を持つようになったことは注目すべき重要なことです。これらの企業は、より多くの潜在的な脅威を軽減しなければなりません。

ドメインセキュリティスコアと「グローバル2000」のランキングの関係

企業の「グローバル 2000」ランクが高いほど、その企業のドメインセキュリティ体制は優れています。



不審なドメイン、あるいは悪意のあるドメインによる「グローバル 2000」企業を標的とした活動

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、標的とな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、その他様々な形のデジタルブランドの乱用、知的財産侵害を意図して行われるものであり、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。

フィッシング詐偽師、また悪意あるサードパーティーが利用できるドメインスプーフィングの手口や組み合わせ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、当社では意図的に注目しています。

ドメインスプーフィングの戦術

あいまい一致

cscg1obal.com　cscgl0bal.com

紛らわしい文字列 - IDN

ćscglobal.com　csçglobal.com

カズンドメイン

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　csccl0bol.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よく検出されるため、よくあるアルファベットの置換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 → 1
s → 5	o → 0	e → 3
l → 1	l → i	w → vv

75% 紛らわしい文字列の75%以上はサードパーティが所有しており、これは2021 年の調査結果と一致しています。

サードパーティ所有ドメインのうち:

82% 2021年の**77%**と比較して、2022年にはその82%がWHOISまたは所有権の詳細を隠しており、プライバシー保護の使用が増えていることを示しています。これは、ドメインの所有や身元を隠すための手段であり、悪意のある意図があることを意味する場合があります。

48% 2022年にMXレコードを所有しており、これは2021年の**43%**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?

46% 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

41% 非アクティブなウェブサイトを所有していた割合

5% 悪意のあるコンテンツを指摘された割合 。不快なコンテンツは、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ります。ユーザーが悪質なコンテンツを含むウェブサイトにアクセスしたり、機密情報が盗まれるリスクがあります。

8% 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

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™ | PDR LTD

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？

フェイクドメインの登録で標的にされている上位の業界

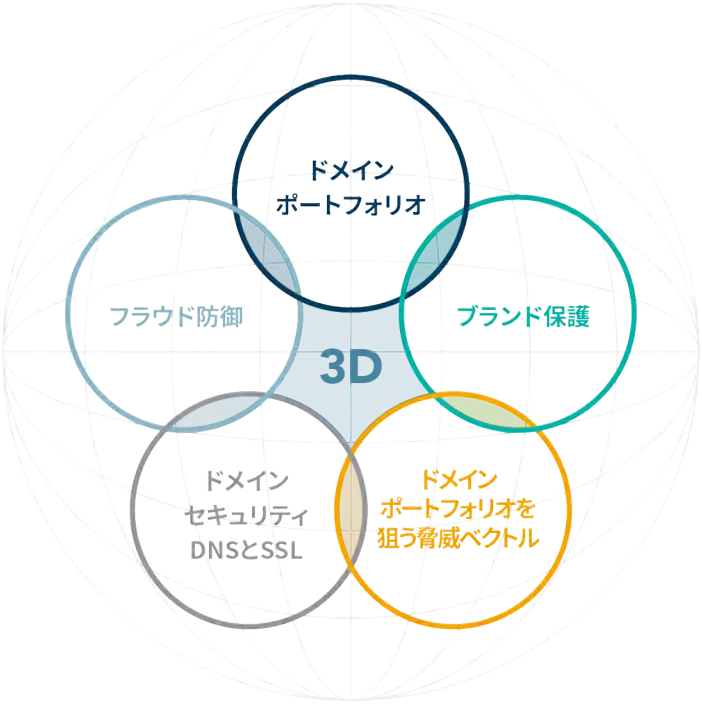
業界	フェイクのドメインの脅威が全体に占める割合
銀行	10.0%
ITソフトウェアおよびサービス	7.0%
企業向け製品・サービス提供	5.5%
耐久消費財	5.4%
医療機器およびサービス	4.6%
統合金融	4.6%
医薬品およびバイオテクノロジー	4.6%
通信サービス	4.5%
輸送	4.2%
保険	4.1%
石油およびガス	3.9%
建設	3.7%
マテリアル	3.5%
食品・飲料・たばこ	3.5%
小売	3.2%
化学	3.2%
テクノロジーハードウェアおよび装置	3.2%
ホテル・飲食・レジャー	3.0%
資本財	2.8%
公益事業	2.7%
航空宇宙および防衛	2.5%
家庭用品・個人向け商品	2.1%
商社	2.0%
複合企業	2.0%
メディア	1.8%
半導体	1.7%
食品市場	0.4%

CSCのDOMAINSEC℠プラットフォームについて

CSCの3D Domain Security and Enforcement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が発明したSaaSサイバーセキュリティプラットフォームで、ブランドのドメインエコシステムの安全維持と防御を目的とした業界初の包括的アプローチです。独自のMachine Learning Deep Search（MLDS）技術を利用したテクノロジーで、機械学習、AI、クラスタリング技術を組み合わせて、侵害の主要な指標を特定します。

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防止ソリューションを一つのプラットフォームで提供します。つまり、私たちは飛躍的に優れた保護を提供し、境界の保護にとどまらず、ゼロトラストセキュリティモデルの改良を支援することができるのです。



結論

企業がドメインセキュリティに対処しない場合、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。この問題に対する認識が高まり、サイバー保険プロバイダが、ドメイン防御戦略とアプローチの品質と厳格さについて、クライアントに責任を求めるようになると予想されます。

企業は、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ために、ゼロトラストのフレームワークの中で階層化セキュリティモデルを必要としています。前述のとおり、このアプローチには、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、ドメイン名やDNSなどの露出したサーフェイスの可視化、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などが含まれます。

ドメインやブランドを サイバー脅威やフラウドから守るために、ドメインセキュリティに関する推奨事項をご覧ください。

CSC

CSCは企業向けドメイン名、ドメイン名システム（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防止サービスのセキュリティおよび脅威インテリジェンスの信頼できるプロバイダとして、フォーブス誌「グローバル2000」や 100 Best Global Brands® 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行っているため、CSCは、企業が、現在存在する既知のサイバーセキュリティの監視を理解するお手伝いをし、オンラインデジタル資産とブランドの保護を支援できます。CSCの特許テクノロジーを活用することで、企業はセキュリティ体制を強化し、オンライン資産とブランドの評判をターゲットとするサイバー脅威ベクトルから保護し、壊滅的な収益の損失や一般データ保護規則(GDPR) などのポリシーによる重大な罰金を回避できます。CSCは、オンラインブランドモニタリングと保護活動を組み合わせたオンラインブランド保護サービスを提供し、フィッシング対策としてフラウド保護サービスと共に、デジタル資産保護に向けた総合的なアプローチを採用います。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、当社がサービスを提供するすべてのビジネスで専門家を雇用し、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す。cscdbs.com/jpをご覧ください。

CSCによるリサーチ:

イハブ・シャイム	最高技術責任者
ヴィンセント・ダンジェロ	戦略的提携とパートナーシップ担当グローバルディレクター
エリオット・チャンピオン	グローバルブランドおよびドメイン担当プロダクトディレクター
クイン・タガート	グローバルブランドセキュリティ担当セキュリティシニアアドバイザー
フェルナンド・セバロス	グローバルフラウド対策および脅威インテリジェンス担当プロダクトディレクター

Copyright ©2022 Corporation Service Company. 無断複製禁止。

CSCはサービス提供企業であり、法的または財務的なアドバイスの提供はしません。本報告書に記載されている内容は、情報提供のみを目的としています。本情報を利用する際には、事前に法律および金融アドバイザーへご相談ください。

DBS11112022