ドメインセキュリティ報告書

フォーブス誌「グローバル 2000」企業

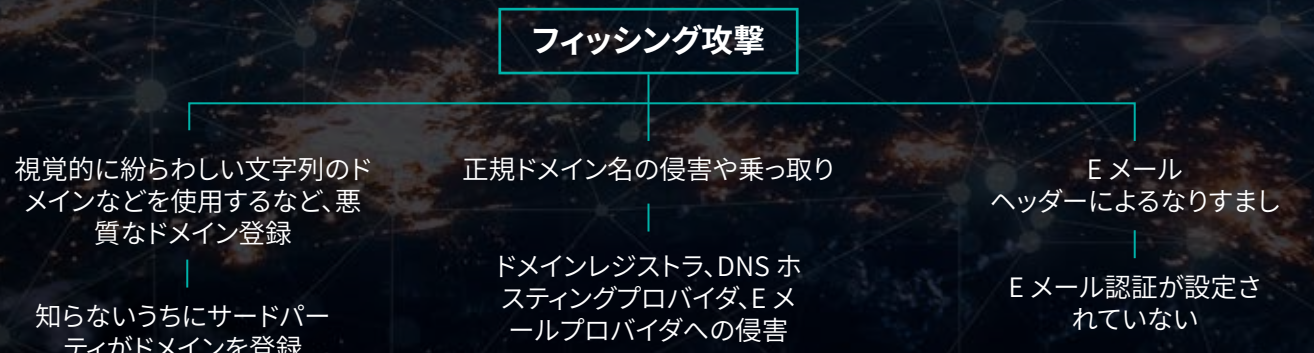
2021

はじめに

サイバー犯罪の増加に伴い、2021 年は企業がランサムウェア攻撃、ビジネスメール詐欺 (BEC)、フィッシング攻撃、サプライチェーン攻撃、オンラインブランドや商標の乱用などの被害に会うケースが増加しています。ドメインに対するサイバーリスクが上昇している一方で、ドメインセキュリティ体制を改善するために、フォーブス誌グローバル　2000」ランクイン企業が取っている行動は変わっておらず、結果としてさらに多くのリスクにさらされる状況となっています。

ドメインセキュリティは、サイバー攻撃を初期段階で低減するための重要な要素であり、*いわば防御の最前線です。*

CISA によれば、ランサムウェアや BEC など大部分のサイバー攻撃は、まずフィッシングから始まります。現在、ランサムウェアによる損失は年間で数十億ドルを超えていますが、ほとんどのランサムウェアに対する防御と対策は、最も一般的なフィッシング攻撃から防御するためのドメインセキュリティ対策が含まれていないため、ランサムウェア攻撃の初期段階であるフィッシングリスクに十分に対応できていないのが現状です。定評のある調査によれば、フィッシング攻撃は主に、悪意に基づき登録された紛らわしいドメイン名や、乗っ取られた正規ドメイン、あるいは E メールヘッダー偽装などを通じて行われます。



ドメインに関するサイバーリスクを理解する

ドメインセキュリティの対策を行っていない場合、破滅的な結果を招く恐れもあります。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。

CSC は、ドメインセキュリティについて、次のようなサイバーセキュリティに関するリスク構造に細心の注意を払うことをお勧めしています:

ドメインセキュリティ構造

主な調査結果

フィッシング詐欺やブランドの乱用の手口としてよく使われる紛らわしい文字列のドメイン（あいまい一致）の 70% は、サードパーティが所有し、一般消費者グレードのレジストラで登録されている。このようなドメインのうち **60%** 以上が過去 2 年以内に登録されたものであり、この攻撃手法が急激に増加していることを示している。

81% は、ドメインレジストリロック手順など基本的なドメインセキュリティ対策を導入していないため、ドメイン名やドメインネームシステム (DNS) ハイジャックのリスクが高くなっている。

57% は、ドメインや DNS のハイジャック、分散型サービス拒否 (DDoS)、中間者攻撃 (MitM)、DNSキャッシュポイズニングに対する防御が不十分な一般消費者グレードのドメインレジストラに依存。

E メール認証方法に、DMARC (送信ドメイン認証) レコードを使用している会社は **50%** に過ぎない。

フィッシング詐欺対策におけるドメインセキュリティの重要性

近年のサイバー攻撃は、主要産業およびソフトウェアプラットフォームで接続しているサプライチェーンを標的としているため、1 つ侵害されると急激に被害が広がる傾向にあります。また、ドメインと DNS は相互接続しているため、前述のドメインセキュリティとドメインレジストラの脆弱性が、インターネットのサプライチェーンのリスクをさらに増大させる可能性があります。積極的かつ予防を重視した制御により、基礎を支えるドメイン資産を保護し、前述のようなフィッシング攻撃の手口から防御することができるのです。そのための必須対策は次の通りです:

- **ドメインレジストラ基準**を用いて大手の企業・機関が消費者向けレジストラを使用する際に潜むリスクを理解することで、フィッシング詐欺やブランドの乱用など、悪意ある目的に利用されやすい業務手法を改善します。
- ドメインレジストリロック、DMARC、DNS ホスティングの冗長性、DNS セキュリティ拡張機能 (DNSSEC)、認証局認証（CAA）レコードなど、業**界全体でのドメインセキュリティ対策を導入**します。
- フィッシングや詐偽行為に利用される、ブランドに類似した**紛らわしいドメインを継続的かつ迅速に検出して無効化**します。

ドメインセキュリティ:
不審な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

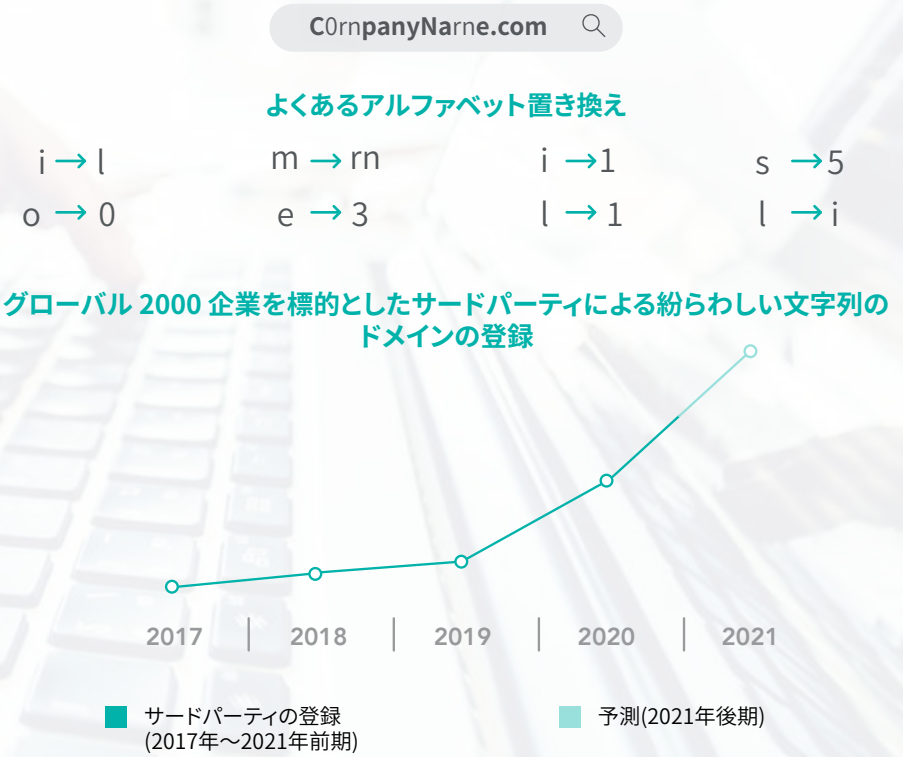
CSC では、「グローバル 2000」企業のブランド名を 6 文字以上含むドメインのうち、ブランド自身が所有していないものを特定し、分析しました[1]。このような不審なあるいは悪意のあるドメイン登録は、標的となるブランドに寄せられる信頼を利用して、フィッシング攻撃を仕掛けたり、その他様々な形のデジタルブランドの乱用、知的所有権侵害を意図して行われるものであり、収益の損失、トラフィックの迂回、正規ブランドの評判失墜につながる恐れがあります。

フィッシング詐偽師や悪意あるサードパーティーが利用できるドメイン偽装の手口や組み合わせは無限に存在しています。

CSC は「グローバル 2000」企業の中核ブランドを標的としたあからさまな手口のうち、悪意あるドメイン登録に関する活動を中心にドメインセキュリティ調査を行うことにしました。

.COM ドメインにおける紛らわしい文字列(あいまい一致)

フィッシング詐偽ドメインでよく検出されるため、調査では、例えば、C0rnpanyNarne.com を使って CompanyName.com のように見せかけるといった、よくあるアルファベットの置換も対象としました。



[1]調査は、サードパーティによる登録が最も多いと予想される .COM 拡張子に範囲を限定して実施されました。また、誤検出を避けるため、堅実かつ有意義な手法を採用し、6 文字以上の中核ブランドを分析しました。

70% グローバル 2000 企業ブランドに類似した登録ドメインのうち、サードパーティが所有していた割合。

サードパーティ所有ドメインのうち:

60% は 2020 年から 2021 年前半にかけて登録が行われており、当社の予測では 2021 年末までに **68%** まで上昇する可能性があります。

77% がドメインプライバシーサービスを利用しているか、WHOIS の情報を編集していました。

これは、ドメインを所有していることや身元を隠すための手段であり、悪意のある何からの意図があることを意味している場合があります。ちなみに「グローバル 2000」企業の正規ブランドは、プライバシーサービスを利用したり、WHOIS の詳細を編集したりしているのは、全体のわずか 25% にすぎません。

43% は MX (E メール) レコードが設定されています。

こういったドメインの半数近くは、フィッシングメールの送信やメール傍受に悪用可能な MX レコードが設定されています。

疑わしいまたは悪意あるサードパーティー所有ドメインで最もよく関連が見られるドメインレジストラを分析対象としています:

GoDaddy.com, LLC **Namecheap, Inc** **PDR, Ltd**

これらサードパーティドメインは、現在どう利用されているのでしょうか?

56% は広告やペイパークリックの Web コンテンツを示すか、ドメインパーキングに利用されていました。

パロアルト社の調査では、ペイ・パー・クリック・ドメインがマルウェアの拡散に悪用されている手口が説明されています。サイバー犯罪者は、休眠状態のドメインを狡猾に利用し、攻撃の準備が整ったときに有効化しているのです。

38% が休眠ウェブサイトを所有していました。

これらのドメインのうち 1/3 には、ネームサーバが設定されていませんでした。これは、ドメイン名が一時的に停止されたことを示している可能性があります。

また、残りの 2/3 のうち、**57%** は有効な MX レコードが設定されていました。

6% は、正規ブランドになりすましたり、フィッシングやマルウェアの配信など、悪意あるコンテンツを示していました。

悪質なコンテンツは、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。お客様が悪質なコンテンツを含むウェブサイトにアクセスしてしまったり、機密情報が盗まれる危険性があるのです。

推奨対策

これらサードパーティー所有ドメインの分析から、その多くがサイバー攻撃を目的とした悪質なドメインとして利用される傾向が高いことが分かりました。登録者は通常、プライバシーサービス利用や WHOIS の編集などにより身元を隠し、有名ブランドに類似した紛らわしいドメインを登録し、エンドユーザにリンクをクリックさせるよう仕向けたり、ブランドの正規サイトを装った偽サイトを信用させる手口を使います。

そこで、企業の皆様にはテイクダウン機能を備えた強力なドメイン・ウェブ・フィッシング詐欺監視プログラムの構築をお勧めします。また、完全一致のドメインを登録し、紛らわしい文字列、あいまい一致、いとこドメイン名などの様々なドメイン偽装の手口から防御し、さらに、新しいジェネリックトップレベルドメイン (gTLD) や、その他のリスクが高い国や拡張子のみならず、事業や販売を展開する国別コードの拡張子も登録しておくなど、全方面に対して対策を取ることができる「360 度ドメイン管理戦略」を確立する必要があります。

ドメインセキュリティ分析

フォーブス誌「グロバール 2000」ランクイン企業のドメイン名セキュリティに対する体制

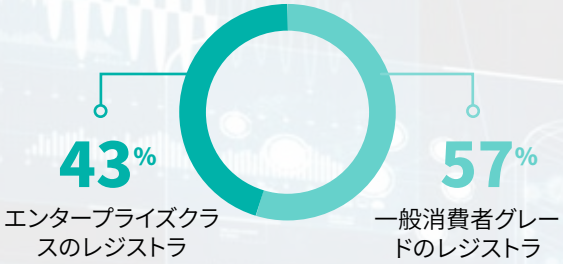
この報告書に記載されている分析はすべて、公表されているデータに基づいており、サイバー犯罪者や国家が背後で操るハッカーもこれらのデータを DNS 攻撃やドメイン名ハイジャックに悪用することができます。この報告書は、これら脅威に対する意識を向上させ、お客様の何社かがすでに導入しているドメインセキュリティに関する最善の対策を広くお知らせすることで、あらゆる企業・機関のドメインセキュリティ体制を強化することを目的に作成されました。CSC は、「グロバール 2000」の全企業について、以下の各ドメインセキュリティ対策導入について分析し、産業および地域ごとの詳細も深く掘り下げて調査しています。

本年度の報告書では、使用しているドメインレジストラの種類に応じたドメインセキュリティの導入傾向についても分析されています。あらゆるセキュリティ対策において、エンタープライズクラスのレジストラを利用している企業の方が、一般消費者グレードのレジストラを利用している企業よりも対策の導入割合が高いことがわかりました。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あり、一般消費者グレードのレジストラのほとんどは、このようなレジストリロックに対応していません。

エンタープライズクラスのレジストラでは、一般消費者グレードのレジストラを利用している場合に比べて、ドメインセキュリティ管理の導入率が平均で 2 倍高くなっています。

当社の調査は「グローバル 2000」ランクイン企業に基づいて実施されましたが、ランクインやランクオフなどによりリスト掲載企業は毎年変化しており、2020 年の対象企業も前年から若干変わっています。

ドメインレジストラのプロバイダ



調査結果

世界有数の企業が名前を連ねる「グローバル 2000」企業の 57% はエンタープライズクラスの大手レジストラを使用していません。一般消費者グレードのレジストラではなく、信頼できるエンタープライズクラスのレジストラがドメイン名ポートフォリオ全体を管理することで、ドメインセキュリティ基準や最善の対策を採用することが可能になります。

エンタープライズクラスのレジストラの主な特徴:

- ☑ 企業専用のドメイン、DNSおよび証明書管理サービスを提供できる企業規模と専門性。
- ☑ サイバーセキュリティと知的財産保護を重視。

  次のようなサービスの提供はしない:
  - 小売サイトや再販業者を介したドメインサービス
  - 知的財産権や商標権の侵害を助長する ペイパークリック、代替ドメイン提案やドメインオークションのサービス
- ☑ ドメインレジストリロック、DMARC、DNSSEC、CAA レコード、DNS ホスティング冗長性など、高度なサービスを通じたドメインセキュリティを重視。
- ☑ 世界および各国各地域での 24 時間 365 日のサポート体制と、世界中のドメイン登録サービスを提供。
- ☑ KYC (顧客本人確認) 手法を用いた顧客情報の収集と検証。
- ☑ ICANN およびレジストリの世界的な認定取得。
- ☑ ドメイン・ブランド・不正行為の、監視・権利行使・不正サイトテイクダウンサービスを提供。
- ☑ ドメイン管理およびセキュリティ、ブランド保護や詐欺行為からの防御を促進する無料のアドバイスサービスや手段 (CSC Security Center℠など) を提供。
- ☑ 書面による依頼の必須化、サイバーセキュリティ意識向上研修の実施、データ・ポリシー対策など、クラス最高の運用プロセスおよび管理。
- ☑ ISO 27001 認定データセンター、SOC 2 準拠、サードパーティーによる侵入・脆弱性試験など、セキュリティを最優先にしたクラス最高水準の運用を実施。

ⓘ 脅威

これまでも、一般消費者グレードのレジストラは、よくサイバー攻撃の標的になってきました。無数のレジストラが、ブランドの乱用や詐欺を可能にしています。(エンタープライズクラスのドメインレジストラを使用するメリットについては、上記をご参照ください)。

レジストリロック

使用しているレジストラのタイプ

52% の企業がレジストリロックを導入するエンタープライズクラスのレジストラを使用

4% の企業がレジストリロックを導入する一般消費者グレードのレジストラを使用

調査結果

驚くべきことに、セキュリティ対策としてレジストリロックを導入する会社はたったの 19% で、「グローバル 2000」企業の 5 社に 4 社は、ドメインセキュリティが非常に危険な状況にあると言えます。世界の企業に対する DNS ハイジャックのリスクが常に存在していることを考えれば、「グロバール 2000」企業によるこの対策の導入率は非常に低い状態です。「グローバル 2000」企業の 43% はエンタープライズクラスのレジストラを使用しており、そのうちレジストリロックを導入しているのが 52%で、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導入率がわずか 4% であるのに比べると、高い導入率を示しています。これにより、使用しているレジストラの種類が、ドメインのセキュリティ管理の導入を左右していることが分かります。

脅威

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。ロックされ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 改ざんやドメイン名ハイジャックにつながる恐れがあります。*また、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いため、一部のドメインがロックされていない状態になることもあります。

DNS 冗長化

使用しているレジストラのタイプ

20% の企業が、DNS を冗長化しているエンタープライズクラスのレジストラを利用

13% の企業が、DNS を冗長化している一般消費者グレードのレジストラを利用

調査結果

「グローバル 2000」企業のうち、中核ドメインの DNS 冗長化 (セカンダリ DNS) を導入しているのはわずか 17% でした。80% を超える企業が、セカンダリ DNS を持たないというリスクを冒しています。従業員や顧客がわずか数分間でも自社ウェブサイトにアクセスまたは取り引きできなくなり、費用が発生するといった脅威は、セカンダリ DNS があれば軽減することが可能です。

脅威

DNS が冗長化されていないと、DDoS 攻撃に対する復旧力が低下したり、ダウンタイムが発生したりするなど、セキュリティに対する脅威となる場合があります。DDoS などの攻撃は、ネットワーク、サービス、アプリなどに大量のデータを送りつけることで、顧客からの正常なアクセスを妨害するため、収益の損失や評判の低下につながる恐れがあります。

DNSSEC

使用しているレジストラのタイプ

7% の企業が DNSSEC を導入するエンタープライズクラスのレジストラを使用

3% の企業が DNSSEC を導入する一般消費者グレードのレジストラを使用

調査結果

DNSSEC (DNS セキュリティ拡張) は DNS サーバー間の通信を認証できる手法の 1 つですが、DNSSEC 導入率は非常に低く、わずか 5% に留まっています。DNSSEC を導入することで、キャッシュポイズニングを防ぐことができます。従ってこの結果は「グローバル 2000」企業の 95% がキャッシュポイズニング攻撃を受ける可能性があるということを意味しています。

脅威

最もコスト効率に優れたセキュリティ手法である DNSSEC が設定されていないと、DNS ルックアッププロセスのあらゆる段階でハイジャックが可能になるなど、DNS の脆弱性につながります。その結果、閲覧セッションが乗っ取られ、ハッカーが詐欺サイトへユーザーをリダイレクトできます。

CAA レコード

使用しているレジストラのタイプ

8% の企業が CAA レコードを導入するエンタープライズクラスのレジストラを使用

4% の企業が CAA レコードを導入する一般消費者グレードのレジストラを使用

調査結果

「グローバル 2000」企業のうち、CAA (認証局認証) レコードを設定している企業はわずか 5% に過ぎません。CAA レコードを設定することにより、会社のドメイン名に関する証明書発行者を特定の認証局に限定できます。そのため、サイバー犯罪者が新しい証明書を取得する際に、指定した認証局を使用しない場合、その要求は承認されず、何者かが CAA ポリシーに適合しない証明書を新たに要求しようとしたという警告が会社に通知されます。これは非常に有効なツールであり、優れたセキュリティを層加えることができます。

脅威

サイバー犯罪者が一旦ドメイン名にアクセスできるようになると、多くの場合デジタル証明書へアクセスするか、新たな証明書を発行します。CAA レコードを追加することで、指定したプロバイダ以外はドメイン名の証明書を発行できなくなります。サブドメイン乗っ取りによる HTTPS フィッシングなどサイバー脅威の低減やポリシー実施の徹底に向けた技術的管理には、CAA レコードの指定が不可欠です。

E メール認証

使用しているレジストラのタイプ

70% の企業が DMARC を導入するエンタープライズクラスのレジストラを使用

44% の企業が DMARC を導入する一般消費者グレードのレジストラを使用

調査結果

DMARC (送信ドメイン認証) の使用率は、現在「グローバル 2000」企業の 50% に達しています。DMARC は、企業のドメインをなりすまし E メールやフィッシング詐欺、その他サイバー犯罪に悪用されるのを防ぐために設計された、E メール認証システムです。DMARC は基本的に、DNS レベルで働く DNSSEC と同じ仕組みで、電子メール認証を行います。また、DMARC レコードが設置されていても、DMARC の拒否ポリシーがないと、フィッシングのリスクが残ることも分かっています。

脅威

なりすまし E メールで、正規の送信元から送られたように見せかけることは非常に簡単です。DMARC や SPF、DKIM などの送信ドメイン認証で E メール経路を認証することで、E メール偽装やフィッシング詐欺を最低限に減らすことができます。

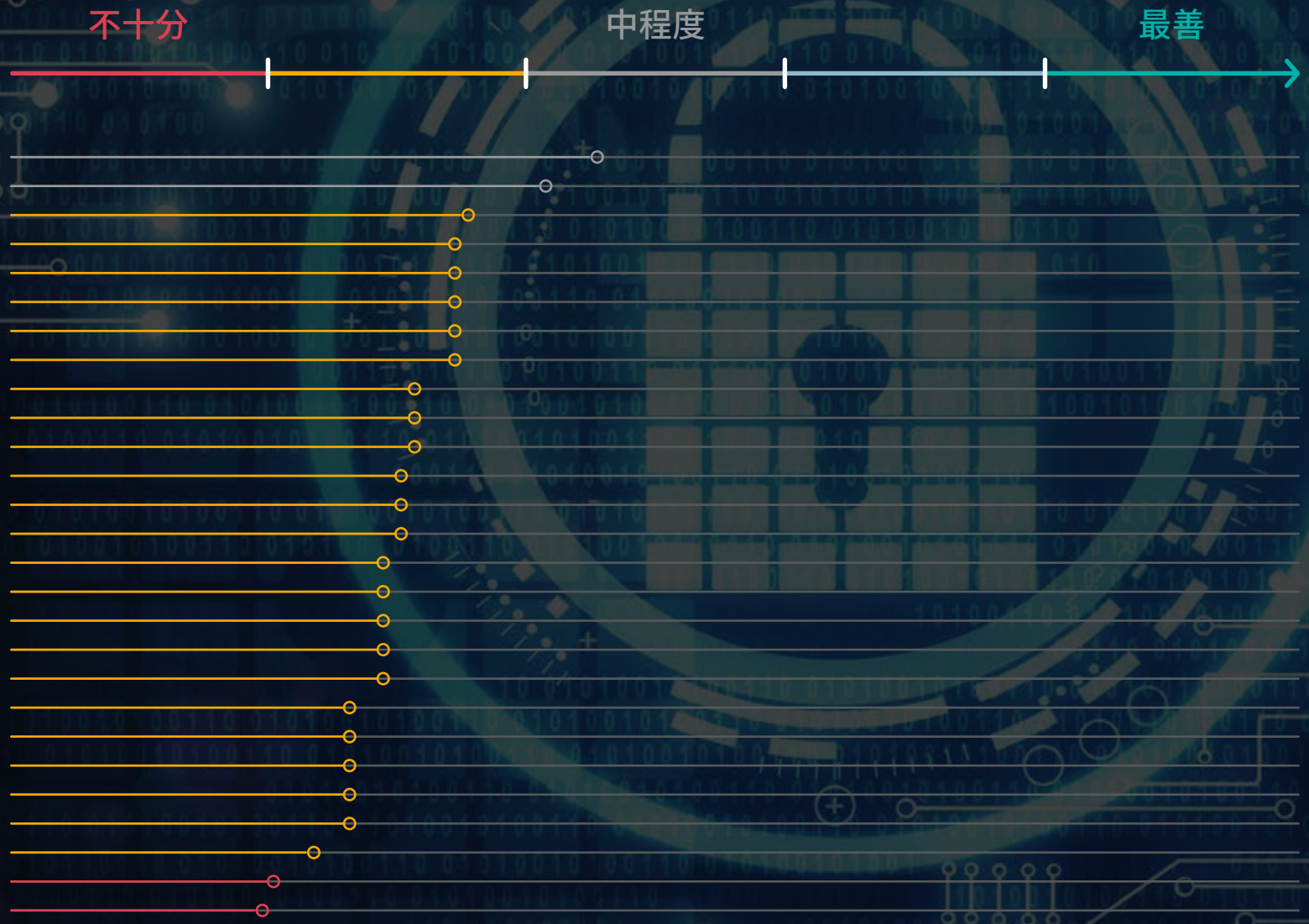
業界別のドメイン名セキュリティ管理の導入

新型コロナウィルス感染拡大の影響で、以前よりも注目されるようになった業界もあります。医療機器・サービス、医薬品・バイオテクノロジー、化学薬品、家庭用品・個人向け商品などですが、これらの業界は、過去 1 年半の間に需要が増加したことで、サイバー犯罪者が狙う主要なターゲットになっています。その中でこういった産業が、リスク低減の有効性という点では依然として中～下位ランキングであることは大きな懸念材料です。これら 4 業界はいずれも、DNSSEC の導入率が極めて低く、医療機器・サービス、家庭用品・個人向け商品では導入率が 0% となっています。CAA レコードも同様にあまり導入されていない状態であり、これは、ブランド企業が知らないうちに、偽装ドメインがデジタル証明書を適用し、正当性を装うことができることを意味しています。またこれらの業界で、ドメイン名のハイジャックや DNS の不正改ざんを防止するレジストリロックを導入している企業は、平均で 4 社に 1 社に留まっています。しかし、これら業界の企業のうち 32～48% が、DNSSEC、レジストリロック、CAA レコードを標準として提供していない一般消費者グレードのレジストラを使用していることを考えると、これら 3 つのセキュリティ手法の導入率が低いことはそう驚くべきことではありません。従ってこれらの企業が、エンタープライズクラスのドメインレジストラと連携することによるメリットは大きいと言えます。

また、米国のエネルギー会社で Colonial Pipelines 社がランサムウェア攻撃を受け、複数の州にまたがる同社の石油パイプラインのうち 約 8,000km が停止に追い込まれた事件以降は特に、石油・ガス業界も注目を集めています。「この事件は、これまでに報告された中で最も破壊的なデジタルランサム攻撃の一つであり、米国のエネルギーインフラがハッカーに対していかに脆弱であるかに注目が集まっている」と、ロイター通信も報道しています。ガス・石油業界はこの事件を深刻に受け止めるべきであり、特に当社の統計によれば、「グローバル 2000」企業の中で、石油・ガス業界は有効性という点で下位ランキングとなっています。この業界の企業のうち、DNSSEC を導入しているのはわずか 4%、レジストリロックを使用しているのは 10% のみです。

銀行業界は、ドメインおよび DNS セキュリティ導入という点では、様々なレベルが混在しています。しかし、間違いなくフィッシング攻撃の主な標的であるこの業界でメール認証手段である DMARC の導入率が 49.7%で、いまだ低い状態なのが気にかかります。

リスク低減の有効性レベル



推奨対策

ドメインセキュリティは、ほとんどのサイバーセキュリティ戦略における弱点となっています。ドメインにクラス最高のセキュリティ対策を適用することで、フィッシング攻撃や ビジネスメール詐欺 (BEC)、ランサムウェア攻撃など早い段階で未然に防ぐことができます。多くの専門家が、強力なサイバー健全性を保ち続けることが極めて重要であると指摘しています。ドメインセキュリティは、企業で十分な対策が取られていない典型的な例と言えます。フィッシング攻撃を防ぐ役割を果たすドメインセキュリティを適用することで、BEC 攻撃やなりすまし詐欺、ランサムウェア攻撃など、多くの脅威を防ぐことができます。

すべての産業のすべての企業、特に新型コロナ感染拡大の影響により注目を集めている企業は、ドメインセキュリティに複数の防御レイヤーで構成される多層防御手法を採用する必要があり、そのためにはまず、エンタープライズクラスのプロバイダを利用することが必要です。CSCは 4 つの重要な戦略を推奨しています:

導入 : ドメイン管理に多層防御手法を取り入れる

確認 : ドメインレジストラの業務手法が、詐欺やブランドの乱用の原因となっていないことをチェックする

継続的な監視 : ブランドの乱用、侵害、フィッシング、詐欺行為がないか、アプリやソーシャルメディア、E メールなど、主要なデジタルチャネルを継続的にモニターする

活用 : 不正サイト閉鎖およびインターネットブロックの高度技術など、包括的な権利行使を実施する

ドメイン管理に多層防御手法を導入

- ドメインレジストラのセキュリティ、技術、プロセス、およびDNS 管理プロバイダを評価することで、サードパーティによるリスクを排除
- 次のような方法で重要なドメイン名、DNS、デジタル証明書を保護:
  - 二要素認証を導入
  - DNS の動きを監視
  - ドメインのレジストリロック、DNSSEC、DMARC、CAA レコード、DNS ホスト冗長化など、各種セキュリティ対策の導入

ブランドの乱用、侵害、フィッシング詐偽、詐欺行為がないか、アプリやソーシャルメディア、E メールなど、主要なデジタルチャネルを継続的に監視

- フィッシング詐偽監視および、ブラウザやパートナー、プロバイダ、SIEM による詐欺防止ネットワークを活用する
- 視覚的に紛らわしい文字列（あいまい一致や外国ドメイン）、いとこドメイン、キーワード一致、同音異義語など、ドメインや DNS の偽装手口を特定
- ウェブコンテンツでの商標や著作権の不正使用を特定
- オンラインマーケットプレイスを監視し、ブランドを乱用から保護
- 関連するソーシャルメディアでのブランドに関するメンションをすべて追跡
- 主要なアプリストアを監視
- 会社へのトラフィックを減らし、ブランドを傷つける不正広告を見つけ、不正サイトを閉鎖

ドメインレジストラの業務手法が、詐欺やブランドの乱用の原因となっていないことを確認

次のような問題は般消費者グレードのドメインレジストラで行われている:

- 商標を含むドメインをドロップキャッチ、オークション、高額入札者へドメイン名を販売するマーケットプレイスで、ドメインを取り引きする行為
- 代替ドメイン名の提案などで、商標を含むドメイン名登録を提案する行為
- 商標を含むドメイン名をペイパークリックサイトで収益化する行為
- DNS 攻撃、フィッシング詐偽、ビジネスメール詐欺などにつながる頻繁な侵 害行為

不正サイト閉鎖およびインターネットブロックの高度技術など、包括的な権利行使を活用

- 知的財産権侵害や詐欺行為に対しては、様々な措置を組み合わせて権利を行使する:
  - 第 1 段階の措置は、オンラインマーケットプレイスからの排除、ソーシャルメディアページの停止、モバイルアプリ排除、違反行為即時停止通告書、不正コンテンツ削除、完全な脅威ベクトル低減など
  - 第 2 段階の措置は、レジストラによるドメイン停止、無効な WHOIS ドメインの停止、詐欺行為の警告など
  - 第 3 段階の措置は、統一ドメイン名の紛争解決ポリシー (UDRP) や 統一早期凍結 (URS) 手続き、ドメイン取得、詳細調査、テスト購入など
- 措置を実施するための幅広い技術的および法的手法を駆使し、個別案件に最適な方法を選択する

業界別セキュリティ対策導入率

導入率が高い　導入率が低い

エンタープライズクラスのドメインレジストラ

ホテル・飲食・レジャー	75%
家庭用品・個人向け商品	68%
企業向け製品・サービス提供	65%
メディア	64%
IT ソフトウェアおよびサービス	61%
化学	57%
小売	56%
医薬品およびバイオテクノロジー	56%
航空宇宙および防衛	54%
半導体	53%
医療機器およびサービス	52%
資本財	47%
輸送	47%
食品・飲料・たばこ	47%
耐久消費財	46%
保険	45%
技術ハードウェアおよび装置	42%
銀行	38%
複合企業	38%
通信サービス	36%
貿易会社	35%
その他金融	35%
公益事業	35%
石油およびガス	28%
建設	24%
材料	22%
食品市場	22%

レジストリロック

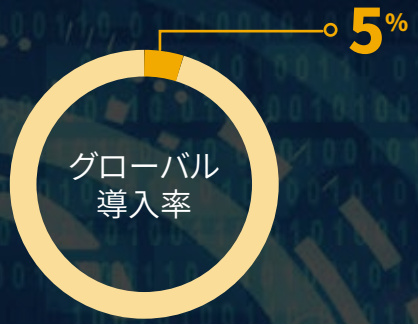
IT ソフトウェアおよびサービス	48%
メディア	40%
航空宇宙および防衛	33%
企業向け製品・サービス提供	33%
半導体	28%
通信サービス	28%
小売	27%
化学	27%
医薬品およびバイオテクノロジー	27%
医療機器およびサービス	25%
耐久消費財	24%
資本財	23%
ホテル・飲食・レジャー	21%
家庭用品・個人向け商品	21%
その他金融	20%
輸送	19%
技術ハードウェアおよび装置	19%
保険	18%
食品・飲料・たばこ	16%
銀行	14%
複合企業	13%
公益事業	11%
石油およびガス	10%
材料	9%
食品市場	6%
建設	6%
貿易会社	3%

導入率が高い　導入率が低い

DNS 冗長化

輸送	28%
石油およびガス	25%
銀行	23%
IT ソフトウェアおよびサービス	23%
航空宇宙および防衛	21%
貿易会社	21%
通信サービス	20%
化学	20%
半導体	19%
保険	19%
小売	18%
その他金融	17%
ホテル・飲食・レジャー	17%
食品市場	16%
資本財	14%
耐久消費財	13%
材料	12%
企業向け製品・サービス提供	12%
メディア	12%
家庭用品・個人向け商品	12%
公益事業	11%
医薬品およびバイオテクノロジー	11%
食品・飲料・たばこ	10%
建設	9%
複合企業	9%
技術ハードウェアおよび装置	8%
医療機器およびサービス	7%

DNSSEC



IT ソフトウェアおよびサービス	14%
航空宇宙および防衛	13%
メディア	12%
銀行	9%
半導体	9%
その他金融	6%
公益事業	6%
企業向け製品・サービス提供	6%
保険	4%
通信サービス	4%
石油およびガス	4%
資本財	4%
耐久消費財	3%
貿易会社	3%
医薬品およびバイオテクノロジー	3%
建設	2%
化学	2%
技術ハードウェアおよび装置	2%
ホテル・飲食・レジャー	0%
医療機器およびサービス	0%
小売	0%
輸送	0%
家庭用品・個人向け商品	0%
食品・飲料・たばこ	0%
複合企業	0%
材料	0%
食品市場	0%

導入率が高い　導入率が低い

CAA レコード

メディア	16%
IT ソフトウェアおよびサービス	13%
石油およびガス	13%
銀行	9%
企業向け製品・サービス提供	8%
通信サービス	8%
複合企業	6%
公益事業	6%
その他金融	6%
化学	5%
技術ハードウェアおよび装置	5%
医療機器およびサービス	5%
ホテル・飲食・レジャー	4%
輸送	4%
保険	4%
材料	3%
小売	3%
医薬品およびバイオテクノロジー	3%
耐久消費財	2%
資本財	2%
建設	1%
食品・飲料・たばこ	1%
半導体	0%
航空宇宙および防衛	0%
家庭用品・個人向け商品	0%
貿易会社	0%
食品市場	0%

DMARC

IT ソフトウェアおよびサービス	74%
医療機器およびサービス	73%
半導体	72%
メディア	64%
ホテル・飲食・レジャー	63%
小売	60%
医薬品およびバイオテクノロジー	60%
石油およびガス	59%
複合企業	56%
通信サービス	56%
技術ハードウェアおよび装置	56%
食品・飲料・たばこ	54%
公益事業	54%
企業向け製品・サービス提供	53%
航空宇宙および防衛	50%
銀行	50%
材料	47%
家庭用品・個人向け商品	47%
輸送	46%
保険	46%
その他金融	43%
貿易会社	41%
化学	41%
耐久消費財	38%
食品市場	38%
資本財	37%
建設	28%

CSC は企業向けドメイン名、DNS、デジタル証明書管理、デジタルブランド保護・ネット詐欺防止サービスのプロバイダとして、フォーブス誌「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。世界的な企業がセキュリティ体制に多大な投資を行っている中で、CSC は企業がセキュリティの盲点を把握し、ドメイン名、DNS、デジタル証明書などを保護できるよう支援しています。CSC　は独自のセキュリティソリューションを活用することで、企業をオンライン資産を狙う脅威から保護し、大規模な収益の損失、ブランドの評判失墜、EU 一般データ保護規則 (GDPR) などの規制による多額の罰金を防ぎます。当社は、オンラインブランド監視と保護活動を組み合わせたオンラインブランド保護、そしてフィッシング対策として詐欺からの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して、オンラインブランド保護サービスを展開しています。

調査および報告書作成: CSC

ヴィンセント・ダンジェロ: 経営企画兼戦略提携担当グローバル部長

ステファニー・ミッチェル: マーケティング責任者

クイン・タガート: シニアグローバルブランドセキュリティアドバイザー

レティシア・ティアン: マーケティング責任者

スー・ワッツ マーケティンググローバルリーダー

cscdbs.com/jp

DBS09172021