
CSC
サプライチェーンの
混乱がドメイン
セキュリティにも影響
cscdbs.com/jp

はじめに

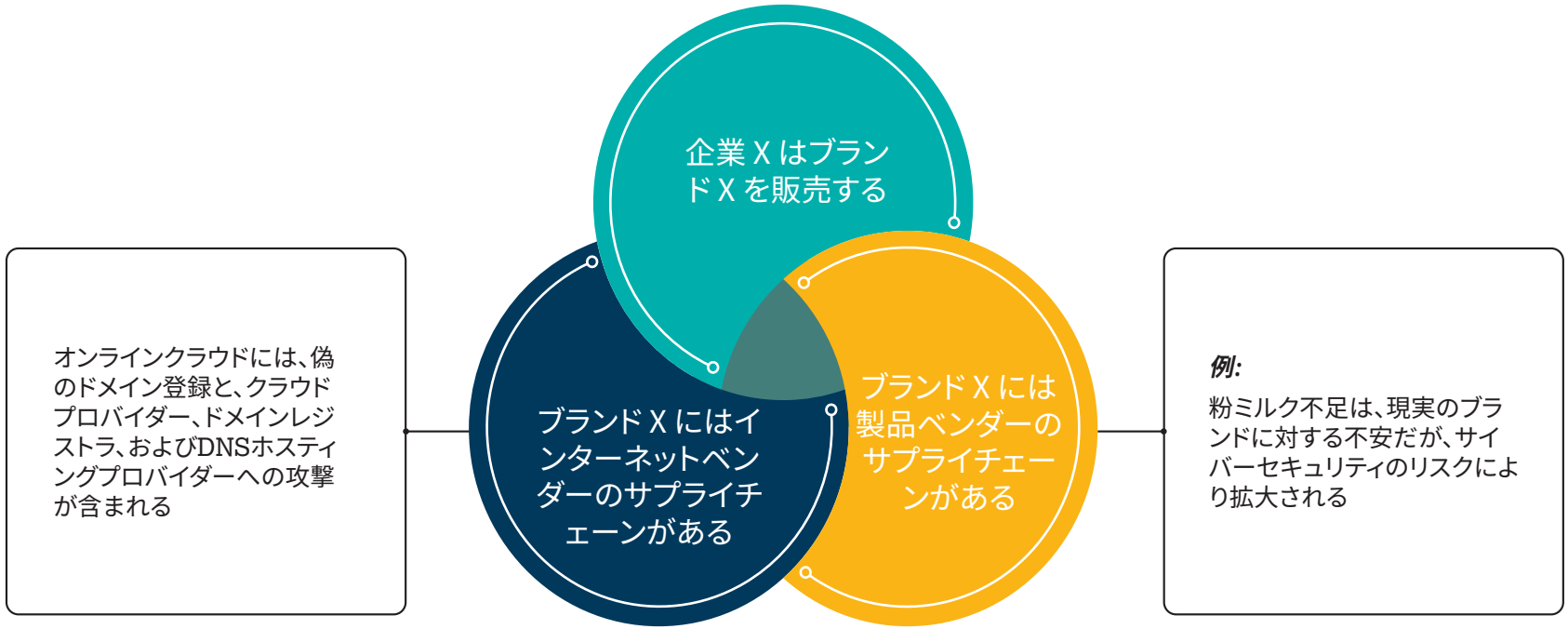
CSC が行った新たな調査によると、模倣品業者が 2022 年の粉ミルクの不足につけこみ、ブランドをかたる偽のドメイン名を利用して消費者をターゲットにしていることが分かりました。主な調査結果によると、信用を築いているブランドを利用し、消費者を正規のウェブサイトとアプリから誘導する粉ミルク関係のドメイン登録が急増しています。2021 年以降に作成されたこれらのウェブドメインのうち **84%** は、ブランドオーナー以外のサードパーティが所有するなどの偽サイトです。これは、製品の安全性、フィッシング攻撃、金銭問題、データ流出などの意味で消費者にとって懸念材料であるだけでなく、これらのブランドを所有する企業にとっても潜在的な問題になり得ます。粉ミルクに限らず、半導体業界で半導体メーカーになりすました偽ドメイン登録も確認されました。2021 年以降に作成された登録ブランドのドメイン名のうち **95%** は、ブランドオーナー以外のサードパーティが所有しています。

最後に、多くの企業でドメインのセキュリティ衛生に問題があり、それがドメインセキュリティのリスクを増大させ、重要なインフラ分野全般に問題が広がっています。クラウドプロバイダーやドメインレジストラに対する大規模な攻撃 (DNS ハイジャックや分散型サービス拒否 (DDOS) 攻撃など)、もしくはソーシャルエンジニアリングやフィッシング攻撃が行われた場合、ドメインセキュリティの衛生を維持することで、これらのリスクに直面して組織の回復力を高めることができるのです。

ドメインセキュリティはサプライチェーンと関連

この 2 年間、これまで考えたこともなかったようなサプライチェーンの品物の供給不足という問題に直面しています。企業の経営陣は、知っておくべきなのに、知らないものはないかと尋ねます。企業にとって重大なリスク要因でありながら、あまり知られていないものがあります—それは、ブランドのウェブドメイン登録のセキュリティです。

コロニアル・パイプライン社や **JBS Foods** など、最近のサプライチェーンに対する攻撃に見られるように、たった 1 つの妥協点を介した 1 つの企業への攻撃は、接続している企業やその製品、パートナー、ベンダー、顧客に至るネットワーク全体に混乱を招く可能性があり、攻撃側には大きな利益をもたらすことができます。ドメイン名と DNS が切っても切り離せない関係性にあることから、ドメインレジストラやクラウドプロバイダーへのたった一つの妥協点、もしくは偽ドメインを使ったフィッシング攻撃が、ネットのサプライチェーンの外にある、製品やインフラのサプライチェーンにまで拡大することもあります。



CSC が行った新たな調査では、供給品不足に影響を受けた企業や消費者のリスクが増加している

偽ドメインは、インターネット上のクラウドの中心地となっており、ブランドオーナーにとっては収益の損失、ブラインドへの中傷、消費者の安全問題、その他サイバーセキュリティ問題を招く可能性があります。CSC は、サプライチェーンの供給品不足など世界的かつ社会的な問題が発生すると、それにつけ込もうとするドメイン登録が増加することを確認しています。CSC は2022 年 1 月、サイバー犯罪者がこれと同様にワクチン関連や医療関係のブランドを悪用し、**新型コロナに関連した不正なドメイン名が急増しているという調査**を発表しました。

CSC の研究チームは、トップの粉ミルクと半導体のブランド名を含む Web ドメインを分析しました。以前の調査と一致して、2021 年から 2022 年 5 月の間に偽のドメイン登録が急増しました。

主な調査結果:
粉ミルク不足

CSC は、粉ミルクの有名ブランド名トップ 5 社、および baby-milk、formula、feed など関連検索語を含むドメイン名を調査しました。

粉ミルクに関連したサードパーティドメイン (ブランドとキーワード) の月間登録件数

84%

のドメインはサードパーティが所有

*当社のサードパーティドメインの定義によると、これらはブランドオーナーによって所有されてはおらず、偽物です。

93% 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、不正な意図があることを意味している可能性があります。

26% は MX (E メール) レコードが設定されています。

MX レコードが設定されたドメインは、フィッシングメールの送信やメール傍受に利用される可能性があります。

当社分析が示す偽の登録に最も関連しているドメインレジストラ:

- GoDaddy.com, LLC
- Sav.com, LLC
- Chengdu West Dimension Digital Technology Co., Ltd

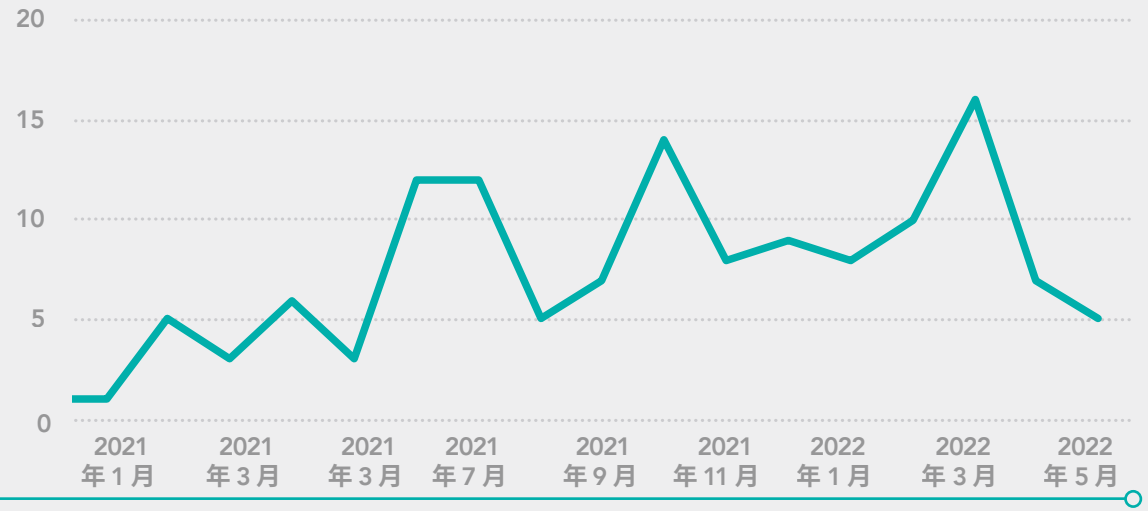
当社分析が示す偽の登録に最も関連している DNS ホストドメイン:

- domaincontrol.com (プロバイダーは GoDaddy)
- bodis.com(プロバイダーBodis)
- registrar-servers.com (プロバイダーは NameCheap)

主な調査結果:
半導体の不足

CSC は、半導体の有名ブランド名トップ 6 や、semiconductor、electronic chip など関連検索語を含むドメイン名を調査しました。

半導体に関連したサードパーティドメイン (ブランドとキーワード) の月間登録件数



95%

のドメインはサードパーティが所有

*当社のサードパーティドメインの定義によると、これらはブランドオーナーによって所有されてはおらず、偽物です。

79% 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、不正な意図があることを意味している可能性があります。

44% は MX (E メール) レコードが設定されています。

MX レコードが設定されたドメインは、フィッシングメールの送信やメール傍受に利用される可能性があります。

当社分析が示す偽の登録に最も関連しているドメインレジストラ:

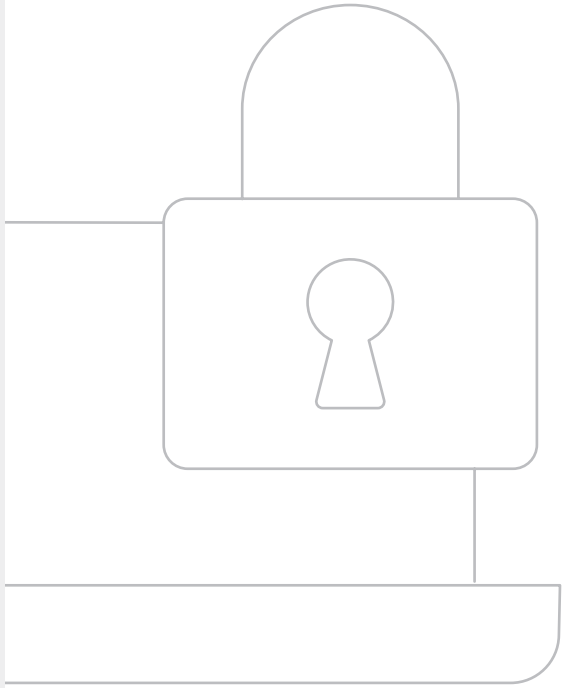
- GoDaddy.com, LLC
- Namecheap Inc.
- Dynadot LLC

当社分析が示す偽の登録に最も関連している DNS ホストドメイン:

- domaincontrol.com (プロバイダーは GoDaddy)
- registrar-servers.com (プロバイダーは NameCheap)
- hichina.com (プロバイダーは Alibaba)

ドメインセキュリティとサイバーの衛生

ドメインセキュリティでは、偽のドメイン登録から企業を保護することはもちろん、**ドメインセキュリティの衛生**の一環として、主要なセキュリティコントロールを積極的に使用することが不可欠です。CSCでは、以下のような高度なセキュリティ対策を取り入れた**多層防御の手法**をお勧めしています。



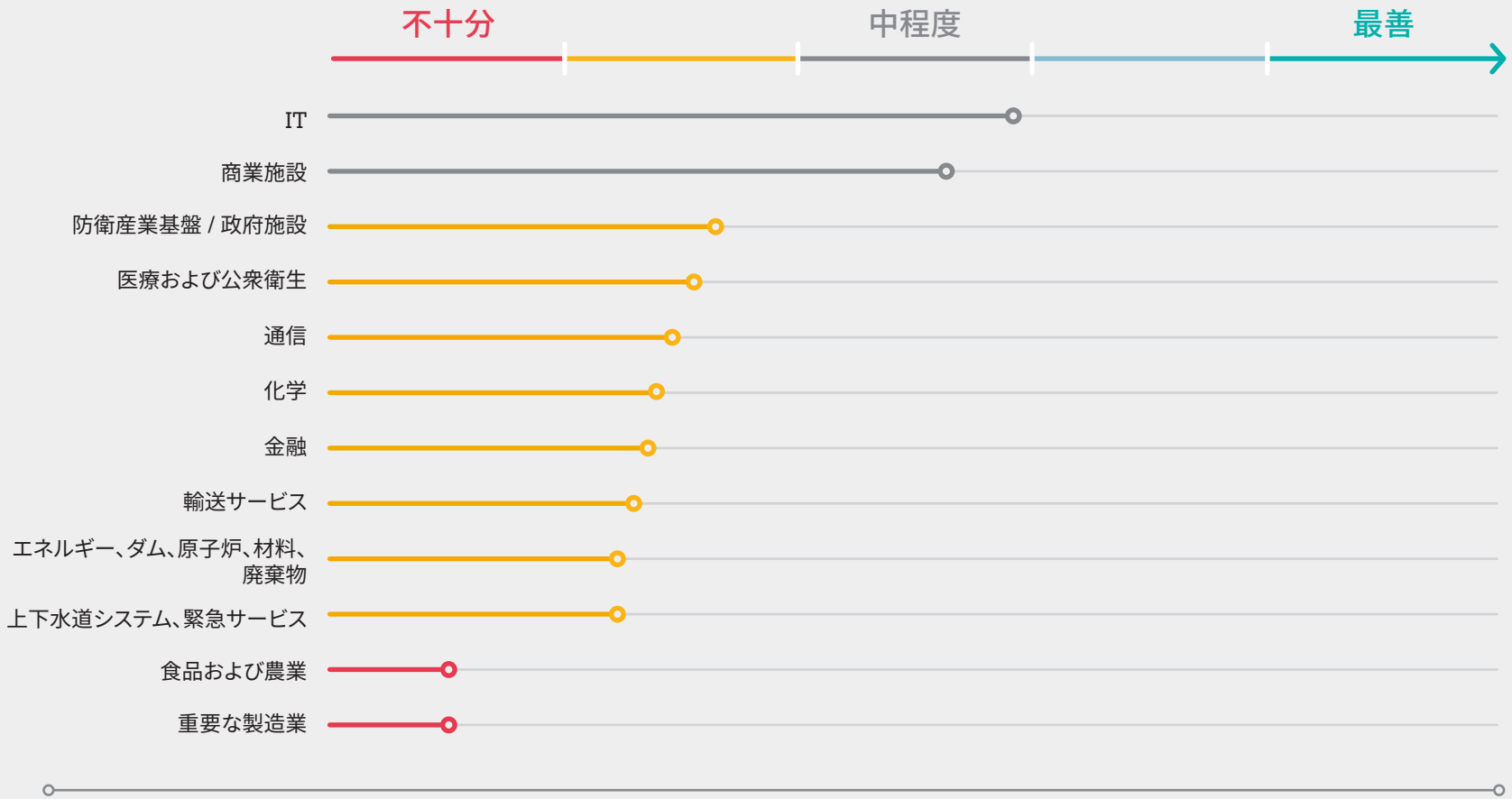
CSC のドメインセキュリティの衛生対策

ドメインセキュリティ対策	目的
DNS ホスト冗長性	ダウンタイムや DDoS 攻撃を低減
DNS セキュリティ拡張機能 (DNSSEC)	ユーザーを怪しいウェブサイトに誘導することを目的とした、ハッカーによるインターネット閲覧セッションの制御を防止
送信ドメイン認証 (SPF)	E メール認証基準は、スパム、なりすまし、およびフィッシングを軽減
送信ドメイン認証 (DMARC)	
送信ドメイン認証 (DKIM)	
MultiLock	レジストリおよびレジストラレベルのロックと WHOIS ロックを組み合わせ、DNS レコードの不正な変更やドメインハイジャックを防止
CAA レコード	証明書を発行する認証局を限定
エンタープライズクラスのレジストラの使用	ドメインおよび DNS 管理、セキュリティ、ブランド保護、クラウド防止、データガバナンス、サイバーセキュリティに関連した、高度なビジネス慣行、能力、専門知識、サポートスタッフを必要とする企業との連携が専門

重要な産業の全体像を把握

CSC の**ドメインセキュリティレポート**のデータを使用して、フォーブス誌「グローバル 2000」企業を調査し、各種の基盤産業を **CISA による重要インフラ分類** 16 項目にマッピングしました。次に、前ページに記載されている 8 つのドメインセキュリティ衛生信号を観察し、これらの重要なインフラセクターでドメインセキュリティ対策をどの程度採用しているかランク付けしました。

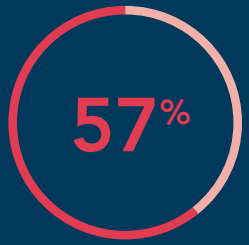
リスク低減の有効性レベル



こういった最新の調査結果により、半導体や粉ミルクを扱う業界 (重要な製造業や食品や農業など) が直面している根本的な大きな問題、つまりドメインセキュリティ体制があまり改善されず、全体的に脆弱であるという点を浮き彫りにしています。

CSC のドメインセキュリティレポート:フォーブス誌「グローバル 2000」企業では、世界で最も重要な産業におけるドメインセキュリティ体制について、詳しい分析をご覧いただけます。

81% は、ドメインレジストリロック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、DNS の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、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。

50% は 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。

リスクが苦し紛れの手段を招き、行動が求められる

品不足になると消費者は、必要なものを手に入れるために様々な手段を取ることになります。ブランドを持つ企業やドメイン業界は、消費者が安全な正規ドメインにアクセスできるように注意しなければなりません。脆弱なドメインセキュリティ体制は新しい問題ではありませんが、より戦略的な重点を必要とする最前線の問題になっているのです。企業は、インターネット上で自社のブランド力の低下や損害につながる、さらに消費者を不正な行為に導く可能性があるものは見つけ出し、排除する必要があります。このようなリスクは回避でき、消費者が必要なものを手に入れようとオンラインを検索した結果、見つけたのはサイバー犯罪者だったといった経験は避けなければなりません。適切なドメインセキュリティ対策を講じ、ビジネスコミュニティが幅広いドメインセキュリティ基準の必要性を知り、導入する必要があります。

ブランドを所有する企業は、DX やブランド保護、サイバーセキュリティのリスク低減のために大きな投資を行ってきました。しかし、ドメインや DNS 内の連鎖的リスクが、サプライチェーンの脆弱性、フィッシング、クラウド (ランサムウェアやビジネスメール詐偽)、ブランドの乱用、偽造を招く結果となっています。重要なインフラを供給している企業は、セキュリティ体制の改善のためできることを実行する必要があります。事業での連鎖的リスクを招くドメインセキュリティはまさにその一つです。

さらに、サイバー保険を提供する業界もこれらのリスクを評価する必要があります。保険会社も保険契約に影響を与える可能性がある新しい指標に目を向け始めているため、企業向けのサイバー保険の保険料や引き受け状況は変わりつつあります。このような指標に反映されているドメインセキュリティ体制の脆弱さは、長期的にもこれらの企業に一定の結果をもたらすことになるでしょう。ドメインセキュリティに関しては、何もしないという選択肢は存在しません。CSC は、幅広いドメインセキュリティの基準、また DNS での毎日の動きや挙動に関した指針や規制が急務と考えています。

お客様の組織の安全を確実に守る方法について詳しくはこちらをご覧ください:

ドメインセキュリティ推奨対策当社のサプライチェーンブログ記事

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ーとして、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。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、現在ある既知のサイバーセキュリティの監視を理解し、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 の専有テクノロジーを活用すると、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、一般データ保護規則（GDPR）などのポリシーによる壊滅的な収益の損失や重大な罰金を回避できます。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。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、クライアントがどこにいてもビジネスを行うことができるグローバル企業です。また、CSC は、当社がサービスを提供しているすべてのビジネスで専門家を雇用してそれを実現しています。**cscdbs.com/jp**をご覧ください。

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

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

スー・ワッツ: マーケティンググローバルリーダー

デビッド・バーネット: コンサルティング責任者、ブランドモニタリング

cscdbs.com/jp

DBS07062022