CSC

IPフロンティア レポート 2025

知的財産権侵害への積極的なセキュリティ対策

はじめに：急激に変化するリスクの高い世界

企業の評判は、オンラインでの表現と非常に密接に結びついています。これにより、詐欺師が有名ブランドを悪用する機会が生まれます。たとえば、偽のウェブサイトを立ち上げたり、製品やロゴをコピーしたり、ブランドを模倣した偽のソーシャルメディアプロフィールを作成することなどです。

なりすましの参入障壁が大幅に下がり、知的財産権（IP）侵害がこれまで以上に容易になっています。知的財産権侵害は特定・追及がますます困難になっており、違反者は、警告書だけでは必ずしも応じるとは限りません。

こうした課題に対応するため、企業は知的財産の執行力を強化し、商標や著作権、その他の権利を守るため、さまざまな戦術を活用することが有効です。

法務部門のリソースが限られている中、マーケティングやIT、セキュリティ部門と連携を深め、知的財産権保護の優先順位を明確にし、予算を適切に配分するにはどうすればよいでしょうか？

「詐欺集団による知的財産権侵害の手口は日々進化しているため、実際に何が起きているのかをより深く理解し、テクノロジーに注力し、ドメイン管理業務に関わる各チーム間でより強固な協力体制を築くことが、すべての関係者にとって有益となります。好むと好まざるとにかかわらず、ドメイン管理はサイバーセキュリティ戦略の重要な要素であり、これは単に重要なドメイン名を保護するだけにとどまりません」とCSCの最高法務責任者であるイアン・マコーネルは語ります。

当社のエキスパート

イアン・マコーネル（Ian McConnel）
CSC最高法務責任者

イハブ・シュライム（Ihab Shraim）
CSCデジタルブランドサービス部門最高技術責任者

エリオット・チャンピオン（Elliot Champion）
CSCグローバルプロダクトディレクター ブランド保護・不正対策担当

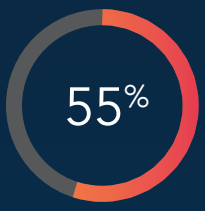
メアリー・ジョー・マーフィー（Mary Jo Murphy）
CSCプロダクトマネージャーブランド・不正対策サービス担当

当社の調査から得られた重要なポイント

2025年第2四半期に300人の上級法務専門家を調査したところ、次のことがわかりました。

オンライン上の知的財産権侵害の発生率は増加しており、今後ますます高まると予測

回答者の大多数（91%）は、オンラインの知的財産権侵害の脅威を懸念していると回答。



半数以上（55%）が、今後3年間でオンラインの知的財産権侵害が大幅に増加すると予想していると回答。

以下が、回答者が経験したオンライン知的財産権侵害の上位3つです：

偽造

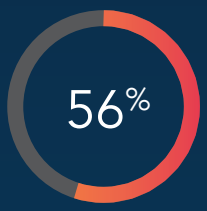
商標の乱用

なりすまし

AIは知的財産権侵害の増加に重要な役割を果たしている

大多数（88%）が、人工知能（AI）搭載システムが侵害の頻度を増加させていると回答。

回答者は、オンライン知的財産権侵害監視のアウトソーシングの利点を認識



半数以上（56%）が、現在一部のオンライン知的財産権侵害監視活動をアウトソーシングしているが、より多くのアウトソーシングを積極的に検討していると回答。

ほとんど企業の法務チームは、知的財産権侵害のリスクを詳細に理解するために、すでにITおよびセキュリティチームと協力中

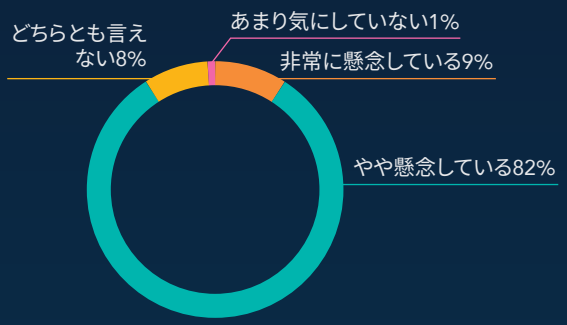
約3分の2（64%）がITセキュリティ部門との連携を「強い」（5点満点中4点）と評価しており、**さらに22%**がITセキュリティ部門と「非常に緊密に連携している」と回答。

知的財産権侵害の発生は増加の一方

過去数年間で、多くの要因が重なり、知的財産権侵害の世界に深刻な影響を与えています。

この多様な推進要因には、サービスとしての犯罪ソフトウェア（CaaS）キットの増加、継続的な生活費の上昇、オンラインショッピングの継続的な成長などがあり、これらすべてが知的財産権侵害を助長し、結果として企業の評判と利益を損なっています。

注目すべきは、CSCのグローバル調査回答者の90%以上が、自組織のような企業に対するオンライン上の知的財産権侵害の脅威を懸念していると回答した点です。



回答者の4分の1は、過去12か月間で自組織が直面するオンライン知的財産権侵害が「著しく」増加したと回答。約3分の1（35%）は過去3年間で「著しい」増加を経験したと述べました。

回答者が最も多く悪用された資産として挙げた上位3つは次の通りです：

- インターネットコンテンツまたはブランドコンテンツ（45%が言及）
- モバイルアプリ（30%）
- オンラインマーケットプレイス（17%）

「人々は、医薬品、自動車部品、消費財など、より安価な製品を常に探しており、詐欺師たちはそれを巧みに利用しています」と、CSCのブランドおよび詐欺対策サービスのプロダクトマネージャー、メアリー・ジョー・マーフィーは述べています。

今後3年間において、回答者の大多数（89%）が知的財産権侵害の増加を予想していると回答。また、10人中9人（90%）が今後12か月間で増加すると予想。

次の種類のオンライン知的財産権侵害のうち、あなたの組織にとって最も懸念されるものはどれですか？

- 偽造
- 商標の乱用
- なりすまし
- 意匠権侵害
- 著作権侵害

「こうした種類の侵害をどう捉えるかは、その人の考え方次第です」とイアンは付け加えます。「消費者向け企業であれば、偽造品が最も懸念されますが、金融サービス企業であれば、詐欺師が商標を不正流用して顧客に対するフィッシング詐欺やサイバー攻撃を仕掛けることの方がより懸念されます。」

> あなたの評判はオンライン上の存在によって示されるため、評判を守るには従来とは異なる方法が必要となります。企業を標的とする脅威ベクトルが大量に増加しており、攻撃者が最も狙いやすいのはドメイン名や知的財産です。過去には詐欺師が何十万件ものフィッシングメールを送り、2〜3%の返信を期待していましたが、現在では不正行為がよりターゲット化され、成功率もはるかに高くなっています。
>
> - **CSCのデジタルブランドサービス部門最高技術責任者、イハブ・シュライム**

知的財産権侵害と戦う上で、ドメイン名を保護することの重要性

ドメイン名は、人々が日々互いに交流し、コミュニケーションを取る方法の中核をなす要素です。あまりにも一般的であるため、人々はドメイン名とやり取りしていることすら気づかず、危険から守られていることを当然のこととして受け入れています。しかし、偽のウェブドメイン名は、深刻な知的財産権侵害の起点となることが多く、詐欺師たちが任意のドメイン名を登録することがこれまで以上に容易になっています」と、CSCのブランド保護および不正防止担当グローバルプロダクトディレクター、エリオット・チャンピオンは述べています。

「最近、QRコードを使って注文できるレストランが増えてきたのにお気付きですか？QRコードをスキャンすると、ドメイン名に直接飛ばされます。どこに接続されるのか全くわからず、ただ信頼するしかないのです」とエリオットは説明します。ドメイン名が、日々のデジタル体験において、いかに重要であるかがわかります。偽りのドメイン名はほんの数分で開設できるにもかかわらず、私たちは皆それらを信じて利用しています。つまり、この種の詐欺行為への参入障壁は今や信じられないほど低くなっているということです。

AIによる知的財産権侵害の拡大

驚異的な速さで、AIは世界のビジネスや生産性の中心となっています。しかしその一方で、詐欺やリスクの観点から見ると、AIはすでに、ロゴ、画像、企業向けコンテンツなど、非常にリアルで高度な知的財産資産を作成するために利用されています。AIやAI主導の能力が急速に拡大する中、法務部門が最も懸念しているのは、リスクをどう検知し、常に最新の状況に先んじて対応できるかという点です。

当然のことながら、調査回答者の10人中9人（88%）が、AI対応システムがインシデントの発生頻度を増加させていると述べています。

回答者の大多数（93%）は、AIを使った偽の資産の生成能力が自社ビジネスに重大な影響を及ぼしかねないと懸念しています。

「今日では、AI活用ツールで架空の資料を簡単に作成し、それを容易に悪用できてしまう時代です」とイアンは述べています。「もはや偽のウェブページをコーディングして作る時代は終わり、ツールがさらに高度になるにつれて、技術に詳しくない不正行為者にとっても悪用の機会がますます増えていくでしょう。詐欺師は自身の想像力次第で何でもできてしまいます。」

企業はAIによってもたらされる新しく進化する課題に直面しています。回答者の10人中9人が、AIツールが自社のデータや知的財産を学習に利用し、競合他社が使えるコンテンツを生み出す可能性を懸念していますが、その懸念を持つ大半は十分な保護策を講じていると考えています。

ポジティブな兆しとしては、多くの企業がAIの脅威拡大を認識し、社内研修や各種取り組みで防御力を高めています。

回答者の約70%が、自社のAIによる知的財産権（IP）資産の作成に関する内部ガイドラインや方針の質を「良い」と評価しており、20%は「非常に良い」と評価しています。

今後、研修が企業のAIリスク予防にますます重要な役割を果たすと予想されます。

事実と虚偽を見分けることはますます困難に

知的財産権侵害に関する懸念事項の上位3つのうちの1つは「なりすまし」であり、その中には、AIによってリアルに生成された経営幹部の偽画像などを利用して、従業員に送金を依頼するケースも含まれています。

「CEOの公開スピーチ、投稿、動画などのコンテンツが十分オンラインに存在しているため、詐欺集団はそれらを使って数時間でAIによる偽の人物を作成できます。その偽物によって社内の多くの人が騙されてしまう」とイアンは語っています。「やがて、普段接している人物と全く同じに見えるオンライン上のなりすましに出くわしても、真偽を見極めるのが困難になるでしょう。

現時点では、偽のビデオチャットを見てもまだ違和感がありますが、その精度は驚異的な速さで向上しており、正直なところ、見極められなくなるのは時間の問題です。

これにより、企業は電話やビデオ、メールなど、個人による認証だけに頼らない仕組みやプロセスを整える必要があります。5年後には、こうした詐欺集団から自身を守るのに有効な研修もなくなるでしょう。

反撃の第一歩は、こうしたコミュニケーションの発信源となるドメイン名の即時削除や、不正な通信の発信元を識別できる適切なプロトコルの導入です。」

予算は増加しているものの、何に使うべきかの優先順位は明確ではない

リスクや要因が増え続ける時代に、IT専用予算はどのように変化して対応しているのでしょうか？

我々の調査によれば、知的財産権侵害やブランド保護のための予算は増加傾向にあり、回答者の3分の2（67%）は今後3年間で「大幅な」増加を見込んでおり、約半数（46%）は今年度に「大幅な」増加を予測しています。

今後12か月間、回答者は追加投資が行われる分野として以下を予想しています：

72%	69%	68%
社内テクノロジー	知的財産管理チームの人員増加	法務部門全体の人員増加

約半数（44%）がCSCのような専門知的財産権委託業者へのアウトソーシング強化を予想。

こうした投資の増加は、「最大の効果を得るためには、資源をどこに投入すべきか？」という重要な疑問を浮き彫りにしています。企業は、すべてのチャネルやドメイン名のバリエーションを網羅しようとするのではなく、本当に成果が出る部分に支出を集中させる必要があります。

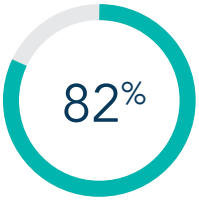
「単に予算を増やすだけでなく、いかにその予算を使うかが問われる」とイアンは語ります。「AI関連の課題に対応するために、どれくらいの費用をかけているか？リスクを適切に軽減するために、必要なリソースの確保にどれくらいの費用をかけているか？」

新たなリスクの急増と、知的財産権侵害のために利用されるチャネルの多様化により、対策は一度きりの取り組みでは不十分で、継続的な分析と監視が不可欠となっています。この課題に対応するため、アウトソーシングパートナーに支援を求める企業が増加しています。

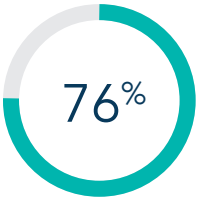
> プラットフォームの変化は非常に速く、私たちが今頼りにしているものもすでに次世代のユーザーが使う新しいものに置き換わりつつあり、それが将来的な主流になります。常に状況は変化し続けていて、追いつくのが困難です。だからこそ、この問題には注意が必要であり、受動的ではなく積極的な対応が求められます。
>
> **エリオット・チャンピオン（CSCグローバルプロダクトディレクター、ブランド保護および不正対策担当）**

知的財産権侵害の対策には、総合的かつ部門横断的な意識が必要です。

回答者は、自社の監視やドメイン管理の戦略について比較的高い信頼感を示しており、大半（86%）がITやセキュリティを含む他部門と密接に連携していると回答。



回答者のが、自社内の知的財産権侵害の監視システムに「非常に」または「かなり」高い自信を持っていると回答。



が自社内でドメイン管理戦略を導入していると回答し、さらに12%が現在策定中だと答えています。

しかし、自社のドメインポートフォリオ管理について法務チームが「完全な」可視性を有していると回答したのはわずか16%でした。

「組織は、特にマーケティング部門が独自ドメイン名でキャンペーンを展開しようとする場合、バックエンドのセキュリティ課題に対応するために一体となったアプローチが必要です」とメアリー・ジョーは述べています。「法務・セキュリティ・ITチームがその実施を事前に把握し、監視リストに追加できるようにしておくことが求められます。」

デジタル・ガバナンスチームの登場

知的財産権侵害対策に積極的で効果的な組織ほど、法務、マーケティング、IT、セキュリティの代表者で構成される正式なデジタル・ガバナンスチームを設置する傾向があります。

「多くの大規模組織では、法務部長とIT部長があまり話をしないことも多い」とエリオットは述べています。「お互いの領域を理解していないのです。私達が新しいクライアントに最初に伝えることは、関係者全員を同じ部屋に集めて、それぞれの視点からこの問題を見てほしいということです。

最も重要なのは、各チームが話し合うことです。月1回程度のミーティングで十分ですが、互いに情報を共有することが不可欠です。」

ドメイン名のモニタリングを含むアウトソーシングサービスの利用拡大

知的財産権侵害の件数が増加する中、ドメイン名やその他関連活動の監視業務を自社のみで管理するのはますます困難になっています。このような業務は、多くの場合、法務部門の責任となりますが、この部門はすでに業務が限界に達していることも少なくありません。

回答者の半数以上（56%）が、現在少なくとも一部の監視業務を外部委託しているが、さらに委託範囲を拡大することを積極的に検討していると回答。

信頼できる実績ある専門企業との提携は、法務部門の負担軽減につながるだけでなく、顧客保護と規制基準遵守への取り組みを示すことにもなります。同様に重要なのは、こうしたパートナーシップがプロトコルや防御体制を強化することで大きな価値を提供すると同時に、新しく革新的なツールやアプリケーションへのアクセスを可能にする点です。

「もしも商標権侵害の訴訟になった場合、以前から商標の不正使用をきちんと監視していなかった企業に対して裁判所は厳しく判断するでしょう」とメアリー・ジョーは述べています。「今日では、CSCのようなパートナーと連携し、市場やマーケットプレイスを監視し、権利侵害を即時削除し、不正行為を極力困難にしていると証明できることが、知的財産権を守るための最大限の努力と見なされます。」

> CSCは、攻撃に使われそうなドメイン名を早めに見つけ出すツールを提供するリーダー的企業です。世界中で高速かつ積極的にこうした活動を展開することで、企業が偽ドメイン名から発生する知的財産権侵害を防ぐことを支援します。
>
> 「責任ある企業が知財侵害の脅威に直面した場合、重層的かつ積極的なサイバーセキュリティ体制が不可欠です。ただファイアウォールを設置すれば十分という時代ではありません。もし知財侵害監視やドメイン管理の外部委託を検討していないのであれば、機会を逸していると言えます。」
>
> **– イアン・マコーネル、CSC最高法務責任者**

一般向けレジストラと企業向けレジストラの違いは何ですか？

一般向けレジストラと企業向け向けレジストラの違いを理解することは、ドメイン名の監視と保護方法を評価する際に不可欠です。イハブは5つの主要な相違点を指摘しています。

1 **執行能力：**企業向けレジストラはグローバルで効果的かつインテリジェントな執行（または削除）を提供しますが、一般向けレジストラにはそれを実現するツールや専門知識が不足しています。

2 **事業焦点：**一般向けレジストラは主にドメイン名販売を目的とした仲介業者であるのに対し、企業向けレジストラはドメイン名の管理・保護とグローバルリスクの軽減に特化しています。

3 **ホストの安全性：**一般向けレジストラはウェブサーバーを提供してドメインをホストすることがありますが、これらは管理が不十分で、安全性の低い共有インフラに依存している場合があります。

4 **セキュリティ体制：**企業向けレジストラは、クライアントのドメインポートフォリオを保護するためにより強固なセキュリティ対策を備えており、一般向けレジストラでは実現できない安全性を提供しています。

5 **監視範囲：**企業向けレジストラは、世界中のECサイトやオークションサイトを監視してドメイン名の不正利用を検出しますが、一般向けレジストラは通常、問題が発生した後にしか対応しません。

「詐欺師は主に3つの手法でブランド所有者を狙います。それは、ブランドの濫用、なりすまし、そして偽造品です」とイハブは指摘。「こうした脅威に効果的に対応するためには、法的執行部門を持つ企業向けレジストラが必要であり、それ以外では十分とは言えません。」

手遅れになる前に行動を

組織の知的財産に対する攻撃は、件数も手口も増加し続けています。AIやCaaS（サービス型犯罪ツール）などの技術により、詐欺師の参入障壁は大きく下がっています。本調査によると、法務の専門家は、これらのリスクに対応するための適切な方針や協働のワーキングプロセスが整っていることに、概ね自信を持っています。しかし、重層的かつ積極的なサイバーセキュリティ体制がなければ、脅威の拡大に対応することはますます困難になります。

信頼できるサードパーティと協力して積極的なセキュリティ体制を構築することで、知的財産の保護に明確かつ有効な道が開かれ、顧客やステークホルダーに対しても適切な安全対策が施されていることを確実に示すことができます。

「積極的に取り組む姿勢は、自分の資産や知的財産を大切にしていることを示します」とメアリー・ジョーは述べています。「最終的には、検知や監視にとどまらず、適切な法的執行や削除対応の体制を整えることによって、確実に成果が生まれます。」

特に経験豊富なサードパーティとの連携による積極的な取り組みは、時間やリソースの面でもより効率的です。

「積極的に対応しないと、その分事後対策に多くの労力が必要になります」とエリオットは結論付けます。「CSCと話せば5分で済むことも、企業向けの専門プロバイダーなしでは、ドメインを取り戻すのに5ヶ月もかかったり、追加費用も発生したりしかねません。」

最後に、イハブは知的財産保護と財務的・評判リスクの関連性の重要さを強調。

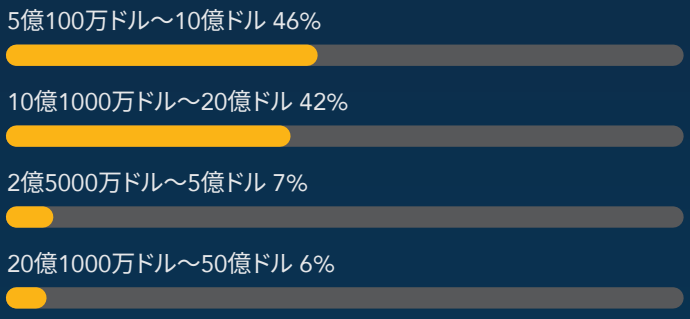
「知的財産権は評判と切り離すことができません。今や企業の評判はオンラインでの存在感に大きく左右されます。」新たな脅威経路が急増している今、従来とは異なる方法で保護する必要があります。」

回答者の概要

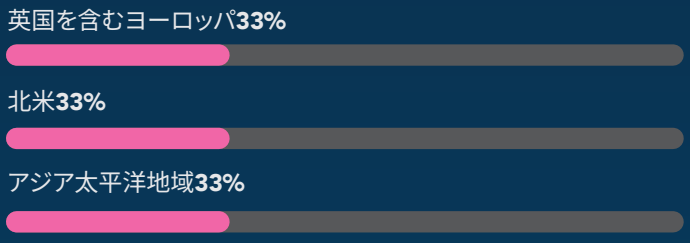
業種別企業数

回答者の役職

企業の年間収益



地域別の企業本社所在地



お気軽にお問合せください

1 800 927 9800 | cscdbs.com

CSCについて

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年より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。cscdbs.comをご覧ください。

DBS10222025