CSC

CSCは企業を陰で支える会社です
（We are the business behind business）

最高情報セキュリティ責任者の展望 2025

AIと規制強化の時代に、進化するドメインベースの脅威を乗り切るために

人工知能（AI）の急速な台頭により、組織に対するサイバーセキュリティの脅威は多様化・激しさを増しています。

今日の悪意のある攻撃者が、ディープフェイクやドメイン生成アルゴリズム（DGA）など、ますます洗練された手法にアクセスできるようになったことで、企業にとって予測と防御がますます難しくなっています。同時に、最高情報セキュリティ責任者（CISO）とそのチームは、分散型サービス妨害（DDoS）攻撃など、より確立されたセキュリティの脅威に対しても引き続き対策を講じる必要があります。こうしたインシデントは、長年にわたる影響抑制のための対策や努力にもかかわらず、依然として企業を危険にさらしています。

2025年第1四半期、CSCは最高情報セキュリティ責任者、最高情報責任者（CIO）、およびその他の上級ITプロフェッショナルを対象とした独自の調査を実施しました。当社は、進化するサイバー脅威、ITセキュリティ予算の現状、サイバーセキュリティの専門家が規制の強化や進化にどのように対処しているか、そしてチームが組織の安全を守るためにセキュリティポリシーやテクノロジーをどのように活用しているのかを理解することを目指しました。

当社の調査の結果、回答者のほぼ4分の3（70%）が、今後1年間にセキュリティの脅威が増加すると考えており、ほぼ全員（98%）が今後3年間で増加すると予測しています。また、ほぼ10人に9人（87%）が、AIを活用したDGAが脅威になると考えています。

> 最高情報セキュリティ責任者が今後も引き続き課題に直面することは疑いありません。当社の使命は、残存するリスクと新たな脅威のベクトルの両方を制御するためのより良い方法を開発し続けることです。

当社のエキスパート

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

ニーナ・フリチャック
(Nina Hrichak)
CSCデジタルブランドサービス部門、EMEAアカウント管理担当

マーク・フレッグ**(Mark Flegg)**
CSCデジタルブランドサービス部門、テクノロジー、セキュリティ製品およびサービス担当

マーク・エグルストン
(Mark Eggleston)
CSC最高情報セキュリティ責任者

最高情報セキュリティ責任者たちの声：スナップショット

2025年第1四半期に最高情報セキュリティ責任者、最高情報責任者、IT部門の責任者300人を対象に調査を行った結果、サイバーセキュリティの脅威は、より困難になっている重大なリスクであることが明らかになりました。

30
人の最高情報セキュリティ責任者が回答

67%
の回答者が、2024年にサイバーセキュリティの脅威が重大または深刻であったと回答。

70%
2025年には脅威が増加すると予測。

98%
今後3年間はリスクが高まると予測。

ドメインとDNSの脅威が主流になると予想

2024年に挙げられたセキュリティ脅威のトップ3：

1. サイバースクワッティング
2. ドメインおよびドメインネームシステム（DNS）の乗っ取り
3. DDoS 攻撃
4. ランサムウェアとマルウェア
5. ソーシャルメディア上のサイバー攻撃と誹謗中傷
6. フィッシングとソーシャルエンジニアリング
7. その他

今後3年間に予想される脅威のトップ3：

1. サイバースクワッティング
2. ドメインと DNS のハイジャック
3. ランサムウェアとマルウェア
4. DDoS攻撃
5. ソーシャルメディア上のサイバー攻撃と誹謗中傷
6. フィッシングとソーシャルエンジニアリング
7. その他

サイバーセキュリティにおけるアウトソーシングサービスの導入は広がっているものの、一貫性が低い

回答者の半数近くが、主に社内のシステムやプロセス、スタッフを利用しており、専門家への委託は限定的であると回答しています。

5分の1弱（18%）がインソースのみで対応しています。

18%

ほぼ3分の1（30%）が専門家に委託していますが、社内のリソースも活用しています。

30%

AIはサイバーセキュリティに大きな影響を与えると予想される

ほぼ10人に9人（87%）が、AIを活用したDGAが脅威になると考えています。

87%

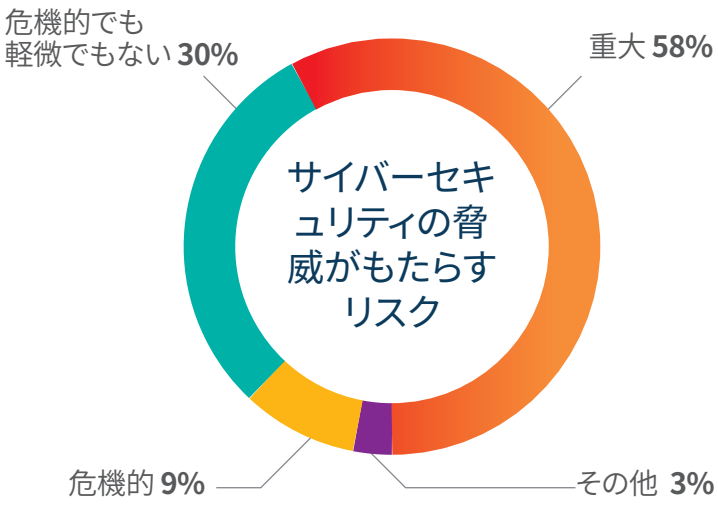
大多数（97%）は、AIベースのサードパーティシステムに企業データへのアクセスを認めることに懸念を抱いていると回答しています。

97%

サイバー脅威は進化し、一層複雑化

最高情報セキュリティ責任者は、ますます巧妙化するサイバー脅威の高まりに直面しています。 しかも、最高情報セキュリティ責任者が直面する安全保障上の問題は、今後ますます深刻化することが予想されます。

回答者のほぼ10人に1人 (9%) が、2024年にはサイバーセキュリティの脅威によるリスクは「危機的」になると回答しました。 5分の3 (58%) がそれらを「重大」と評価し、 3分の2 (67%) がリスクは「実質的」であると回答しました。 また、30%はリスクが「危機的でも軽微でもない」と回答しました。



「最高情報セキュリティ責任者は大きな移行期に対処する必要があったため、リスクをそれほど深刻に感じているのは当然です」と、CSCデジタルブランドサービス部門の、テクノロジー、セキュリティ製品およびサービス担当シニアディレクターの マーク・フレッグ は述べています。

「組織がコアシステムを社内のオンプレミスのインフラストラクチャからクラウドに移行し始めたことで、IT 環境は新たな脅威にさらされるようになりました。 その典型的な例が、サブドメインハイジャック、つまりサブドメインの乗っ取りです。20年前は、企業が自社でデータセンターを運営し、IPアドレス空間やDNS制御を第三者に委託することはほとんどなかったため、この問題はそれほど懸念されていませんでした。 現在、ITシステムへの侵入はより容易になり、悪意のある行為者が、防御の隙を突く機会を常に狙っています。」

サイバー脅威によるリスクは、今後数ヶ月、数年間でさらに深刻化すると、回答者は述べています。 ほぼ4分の3（70%）が2025年に増加すると予想しており、そのうち5%はその増加が「顕著」になると回答しています。98%が今後3年間で増加すると予想しており、そのうち3分の2（66%）はその増加も顕著になるだろうと回答しています。

強力な能力を持つAI技術の台頭は、数々のドメイン関連の脅威がより強力になっていることを意味します。

例えば、サイバー犯罪者はAIを使用して、放棄されたサブドメインや設定ミスのあるサブドメインを驚異的な規模でスキャンし、サブドメインの乗っ取りを成功させる可能性があります。

一方、最高情報セキュリティ責任者が直面する大きな課題は、これまで対応してきた脅威のほとんどが依然として問題となっている中、新たな攻撃や手法のリストが量・複雑さともに増え続けていることにあります。

サイバー脅威はますます巧妙化しており、成功の可能性を高めるために複数の手法を組み合わせて使用することが多くなっています。 多くは、何らかのソーシャルエンジニアリングから始まり、信頼性を高めるために、タイポスクワッティングなどの類似ドメインという戦術と組み合わせる場合もあります。

これらの攻撃は、将来の脅威の土台となり、その実現を可能にする役割を果たしています。

その他の例としては、セキュリティ対策を回避し、ネットワークを介してマルウェアを送信するためのDNSトンネル、またはサードパーティサプライヤーのシステムを侵害し、そのアクセス権を利用して企業のデータを盗むことが挙げられます。

> 「私たちが目にしているのは、ランサムウェアなどの攻撃は単独で発生することはなく、悪意のある行為者がハイブリッド攻撃や複合攻撃で情報を盗み出し、甚大な被害をもたらす可能性があるということです」

マーク・エグルストン（Mark Eggleston）
CSC最高情報セキュリティ責任者

ドメイン関連の脅威が最高情報セキュリティ責任者の懸念事項の大半を占めています。

昨年、サイバースクワッティング、ドメインおよびDNSハイジャック、DDoS攻撃が、セキュリティ上の脅威のトップ3を占めました。

「適切なツール」を導入していると答えたのはわずか22%でした。最高情報セキュリティ責任者は、ドメインベースの脅威に対抗するためにさらに多くのことを行うことが可能だと感じているのは明らかであり、リソースを強化する必要性もより高まっています。

76% 4分の3は、ドメイン攻撃を防ぐ自社の能力について「ある程度自信がある」と答え、「非常に自信がある」と答えたのはわずか7%でした。

99% さらに、ほぼ全員（99%）が、ドメイン登録機関が顧客やサプライヤーの身元を確認するための顧客本人確認手続き（KYC）に関するポリシーを遵守していないことを「多少懸念している」または「非常に懸念している」と答えています。

59% ほぼ5分の3（59%）は、自社でドメインに関連するサイバー脅威を検出した場合、それを軽減するためのツールとプロセスを導入しているが、脅威を排除するのは複雑で時間のかかるプロセスであると回答しました。

当社が行った「最高情報セキュリティ責任者の展望 2025」の回答者の4分の3は、攻撃対象領域やデジタル資産を標的とするデジタル脅威を管理するために、信頼できるDNSプロバイダーを利用しています。

50%がインシデント対応計画を策定し、定期的にテストを実施しており、50%がAIベースのモニタリングおよび執行ソリューションを使用しています。

信頼できるDNSプロバイダーをデジタル脅威の管理に利用している

インシデント対応計画を策定し、定期的にテストしている

AIベースのモニタリングおよび執行ソリューションを使用している

「セキュリティ上の最大のリスクは依然として人的要素であり、どの企業においても、チーム内の教育不足が最大の弱点となっています。DNSハイジャックやサブドメインの乗っ取りは、最近ようやく認識され始めたリスクです。」

ニーナ・フリチャック（Nina Hrichak）

CSCデジタルブランドサービス部門、EMEAアカウント管理担当バイスプレジデント

AIは
サイバー脅威との闘いにおいて
大きな役割を果たしている一方、
広範な利用は引き続き懸念要因

AIが世界中の組織に価値を生み出していることは間違いありません。当社が話を聞いた最高情報セキュリティ責任者やその他の経営幹部は、AI統合における最大の投資収益率（ROI）はプロセス自動化であるとし、その次に社内教育とデータ分析が挙げられました。

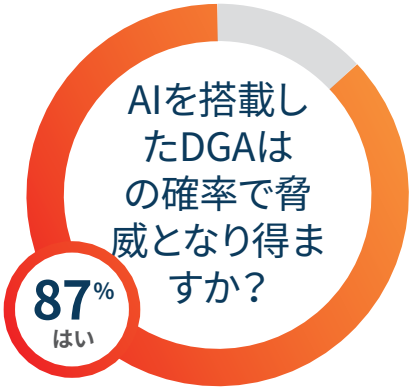
1. プロセスの自動化
2. 社内教育とスタッフ研修
3. サイバーセキュリティ
4. 詐欺検出
5. データ分析
6. クエリー応答

しかし、AI はセキュリティの世界では明らかに両刃の剣と見なされています。その理由の一つは、従業員やベンダーがChatGPTのような大規模言語モデル（LLM）に機密データをアップロードする脅威が生じるほか、サイバー犯罪者がAIを活用してDGAなどのツールを強化する可能性があるからです。

「AIは、研究をより迅速に進めるのに役立つため、良い目的に活用できます。例えば、背景調査を行うには最適な手段ですが、エラーのリスクがあるため、人間による検証なしにGenAIの資料を他者に渡してはなりません」とマーク・エグルストンは説明し、「また、AIはフィッシングに使用されるディープフェイクなどの新たな脅威を生み出す手段としても活用できることを認識しておくことも重要です」と付け加えています。

回答者は、AIベースのサードパーティシステムに企業データへのアクセスを付与することのリスクについて、ほぼ全員が懸念を寄せています。

大多数（87%）は、AIを活用したDGAが自社に脅威をもたらすと回答しました。脅威アクターは、知的財産権を侵害したり、偽造品を販売したり、フィッシング詐欺を支援したりする新しいドメインを大量に生成することができます。ドメインに利用されるキーワードの組み合わせは、無限に近いと言えます。



AIの利用は、説得力のあるメッセージ、偽のウェブサイト、自動化ツールなどを駆使した、組織を攻撃するための完ぺきなキャンペーンを構築・実行にも役立ってると、イハブは警告しています。

「金融サービスなど、特定の業種を標的とした悪意のあるキャンペーンを展開することを可能にする、AIを活用したさまざまなプラットフォームが存在します」とイハブは述べています。「これらのツールキットは、攻撃をより説得力のあるものにするために、包括的に設計されています。かつてよく見られたスペルミスや文法ミスは、AIが高度に正確で洗練されたメッセージを生成できるようになったため、ほとんど見られなくなりました。」

組織は、組織内で誰がどのLLMにアクセスし、どのような情報を共有しているかを明確にしたガバナンスポリシーを策定する必要があります。これには、従業員やベンダーによるAIツールやアプリケーションの無許可使用といった、「シャドーAI」の 脅威の高まりを認識することも含まれます。

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・シュライムによるエキスパートの見解

ドメインに関連する脅威がますます深刻な課題となっている理由

「DNSおよびドメイン関連のインフラストラクチャは、サイバー犯罪者にとって攻撃の標的となりやすい脆弱な部分です。サイバー犯罪者は、DNSハイジャックやドメインスプーフィングなどの特定の脅威ベクトルを利用して、露出しているシステムを悪用します。

悪意のある攻撃者は、ソーシャルメディアから求人サイト

まであらゆるものをスキャンして、フィッシング攻撃に反応しやすい不満を募らせている社内関係者など、潜在的な脆弱性を特定するために広範な偵察活動を展開します。

彼らは、DNS、ウェブサイト、メールゲートウェイなど、組織が公開しておく必要のある資産に焦点を当て、サイバースクワッティングやDNSキャッシュポイズニングなどの精密な攻撃を容易に実行できるようにします。

「すでにこのような攻撃が大量発生しており、2025年には、既製のツールや攻撃キットが広く利用可能になるにつれて、その数は大幅に増加すると予想されます。」

イハブ・シュライムが選ぶ、AIガバナンスポリシーを確立するためのトップ5の対策

1 **明確なAIポリシーを確立する**
AIを導入する組織にとって最優先事項は、正式なポリシーを策定し、社内に周知徹底することです。

2 **データ共有に関する明確なルールを設定する。**
従業員がLLMに入力できるデータとできないデータの種類を明確に定義し、情報漏えいのリスクを最小限に抑えます。

3 **隔離された環境を使用してテストを行う。**
従業員がLLMに入力できるデータとできないデータの種類を明確に定義し、情報漏えいのリスクを最小限に抑えます。

4 **具体的なユースケースを定める**
AIモデルは、特定の機能を自動化するなど、明確な目的を持って構築する必要があります。これにより、意図しないデータ汚染を防ぐことができます。

5 **AIの生成結果を検証する**
AIを使用する者は、AIが生成したデータが普遍的に正確であるとは想定すべきではありません。人間のチェックは依然として不可欠です。

「相互に接続されたAIモデル間で情報が繰り返し強化されることで、インターネットのセグメント全体が偽のデータで汚染される可能性があります。将来、技術者が使用するデータの基礎的なチェックを行うことは、さらに困難になるでしょう。」

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

シャドーAIに
焦点を当てる

ある意味で、シャドーAIは、エンドユーザーがITガバナンスを迂回する場合に最高情報セキュリティ責任者が直面する、長年にわたる一連のセキュリティ脅威の最新の例とみなすことができます。これは、従業員がDropboxなどのツールを初めて利用し始めた時や、監督のないまま自分のモバイルデバイスを職場に持ち込んだ時と似ています。

また、別の見方をすれば、シャドーAIははるかに複雑で、より悪質な脅威です。多くのAIツールはクラウドベースであり、外部でホストされているため、悪意のある行為者はそれらを悪用して脆弱性を発見したり、従業員が意図せずに使用したデータを悪用したりする可能性があります。こうしたリスクには、不正使用によって機密性の高い会社情報や顧客情報が漏洩した場合のデータ侵害やコンプライアンス違反などが含まれます。

マーク・エグルストンによると、シャドーAIの問題に対する解決策は、組織全体で使用されているすべての LLMを追跡するソフトウェアエージェントを利用することです。「つまり、AIツールから情報をアップロードおよびダウンロードしているユーザーを確認し、リスクの高いユーザーをブロックすることができます。次に、ゼロトラストフレームワークを適用してユーザーを検証し、制御を執行することで、全員が組織のAIガバナンスポリシーを確実に遵守するようにします。」

ITセキュリティの予算は、拡大するサイバー脅威の動向に追いついていない可能性があります。

サイバーセキュリティは、大企業にとって最優先の経営課題のひとつと認識されていますが、拡大する脅威や企業が管理しなければならない膨大なデータセットから保護するために必要な予算を確保することは、依然として困難な場合があります。

「問題は、サイバーセキュリティへの投資から目に見える投資収益率が得られないことです」とマーク・フレッグは述べています。

「それは保険に加入するようなものです。誰も保険料を支払うことは嫌がりますが、保険金請求時には、その保険は最高の投資だったと感じるものです。予算重視の企業は、セキュリティ対策のコストが本当に妥当であるかを依然として疑問視しています。」

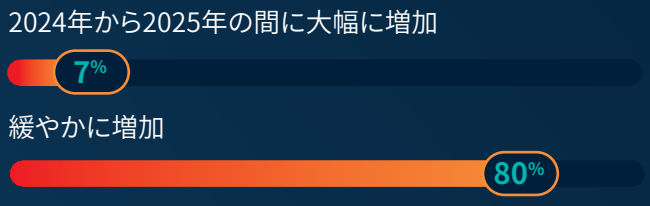
「毎年、より高い予算を計画しておく必要があります」とマーク・フレッグは付け加えます。「これまで対応してきた脅威は、そう簡単に消えるものではありません。そのため、それらに対する資金に加え、新たに発生した脅威に対する資金も確保しておく必要があります。最高情報セキュリティ責任者たちは、ファイアウォールの構築に多くの時間を費やし、城の跳ね橋を引き上げてきましたが、いまや人々が堀の下にトンネルを掘っていることに気づき始めています。」

取締役会におけるサイバーセキュリティの優先順位と資金調達の間に乖離がある理由の1つは、ドメインセキュリティのリスクに関する意思決定が、その潜在的な影響を最もよく理解している者によって行われるとは限らないことです。

最高情報セキュリティ責任者たちは、ドメイン関連の脅威が現実の世界に与える影響について検討し、このギャップを埋めるための措置を講じています。また、多くの最高情報セキュリティ責任者は、上級社員と協力し、脅威についてより深い理解を得るよう努めています。

サイバーセキュリティおよび関連する情報セキュリティと管理に関する全体予算。

2024年から2025年にかけて、サイバーセキュリティおよび関連する情報セキュリティと管理に関する全体的な予算が大幅に増加したと回答した人はわずか7%に留まり、過半数（80%）は予算が緩やかに増加したと回答しました。



サイバーセキュリティの予算配分を決定する責任は誰にあるか？

割り当ては、最高リスク責任者（CRO）またはリスク管理チーム（23%）、CFOまたは財務チーム（21%）、

最高情報セキュリティ責任者またはITチーム（18%）によって決定される場合が最も多い。

最高情報セキュリティ責任者がデジタルリスクに関して他の部門と議論するトップ5のトピック：

1. 評判および経済的損失
2. サイバーセキュリティおよびデータ保護
3. 戦略的計画と事業目標
4. 予算編成および資源配分
5. コンプライアンスおよびリスク管理

“コンプライアンスは、通常、サイバーセキュリティ戦略の中で最も容易な部分ですが、評判や財務リスクに重点を置く最高情報セキュリティ責任者たちが増えているのは良い傾向です」と、マーク・エグルストンは述べています。「ほとんどの最高情報セキュリティ責任者はコンプライアンスの扱い方を理解していますが、評判の失墜は私たちにとって最大の悩みの種です。

ドメインセキュリティの予算が軽視される理由

「多くの企業は、ドメイン名を純粋に商標の予算項目として捉えていますが、この考え方はセキュリティの観点にシフトさせる必要があります」と、ニーナは述べています。

「企業のドメインポートフォリオに関しては、2つの点を留意する必要があります」と彼女は指摘します。「まず、ドメイン名の登録は比較的安価です。第二に、多くの法的管轄区域では、登録に関する規則がほとんどまたはまったく存在しません。そのため、コア市場だけでなく、リスクの高いドメイン拡張子においても、ドメイン登録によるブランドの保護が非常に重要になります。

「ドメインに割り当てるセキュリティ予算を増やすべき理由はここにあります。最高情報セキュリティ責任者がデジタル資産の管理状況を把握できず、セキュリティにあまり重点を置いていない担当者がその責任を担っている企業では、レジストリのロックなどの重要かつ費用対効果の高い対策が見過ごされてしまう可能性があります。

「すべてに通用する万能の解決策はありません。企業は、広範に登録することで防御的な戦略を立てることもできますし、侵害を監視し、必要なときに行動を起こすという無駄のないスタイルを採用することもできます。」

NIS2のコンプライアンスは多くの組織において**依然進行中の取り組み**

規制の遵守は、最高情報セキュリティ責任者にとって常に課題となっています。ネットワークおよび情報セキュリティ指令2（NIS2）や一般データ保護規則（GDPR）などのコンプライアンス違反は、多額の罰金や評判の低下というリスクを伴います。

それにもかかわらず、NIS2は自社には適用されないと判断したり、欧州連合（EU）加盟各国で新法の地域的バリエーションの導入が遅れているため、NIS2を後回しにしている企業も少なくないでしょう。

このような遅れが、回答者が特定のサイバーセキュリティおよび情報セキュリティのリスクに対処する上での困難度に基いて、次のような規制の枠組みをランク付けした要因であると推測されます：

1. NIS2 **（欧州）**

2. GDPR **（欧州）**

3. サイバーセキュリティの成熟度モデル認定 **（米国）**

4. 国際標準化機構、国際電気標準会議 **(ISO/IEC) 27001/2 （世界）**

5. ペイメントカード業界データセキュリティ基準 **（米国）**

6. 重要インフラ保護 **（CIP）基準 （米国）**

7. デジタルオペレーショナルレジリエンス法 **（DORA） （欧州）**

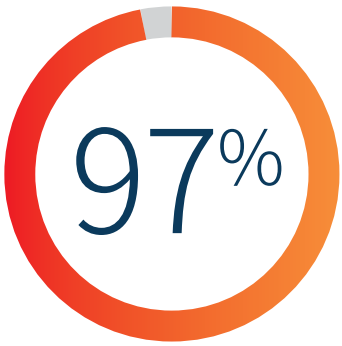
「この指令を文字通りそのまま採用する国もあれば、自国の状況に合わせて適応させる国もあるでしょう」と **マーク・フレッグ** は述べています。「現時点では、各国がこれまでNIS2を実施してきたさまざまな方法の中から、共通点を見つけることしかできません。」

自社の組織がNIS2に完全に準拠していると回答したのはわずか9%でした。最大の課題は、外部パートナーのコンプライアンスの確保（73%）と、複雑な規制を正しく理解し、実施することの難しさ（64%）です。

これは、本レポートの前半で、回答者が、パートナーがサプライヤーやその他の第三者に対するKYCチェック（本人確認）を完了していないことを懸念している、という調査結果と一致しており、こうした慣行は組織のサプライチェーンの安全性に影響を与える可能性があります。

「NIS2が1位になった理由は、現時点で対応が最も急を要する課題だからだと私は考えています」とニーナは述べています。「GDPRが施行されたときと同様、皆、何か行動を取る必要があることは理解しているが、どこから手をつければよいのかまだ完全には把握できていない状況です。一方、ISO/IEC 27001/2はより長い歴史があり、認証を取得するには非常に厳しいプロセスを経る必要があります。」

今後3年間で、御社が直面するセキュリティ監査や規制・コンプライアンス要件の量が増加すると予想されますか？



セキュリティ監査の強化に備える

マーク・エグルストンは、企業が現在直面している規制要件の増加は、AI規制について、これまでデータプライバシー法で示してきたのと同じ傾向、つまり独自の枠組みの開発を優先する傾向が、各管轄区域で顕著になっていることが一因であると指摘しています。

「それを管理する方法は、プライバシーであれ、AIであれ、その他であれ、規制に関連するすべてのデータを1つの制御フレームワークにマッピングすることです」

とマーク・エグルストンは述べています。「つまり、最高情報セキュリティ責任者が監査を実行する場合、すべての基準に対して認証を行うことができます。『一度の監査で複数の認証を行うこと』ができるため、必要な作業が大幅に削減できます。」

「最高情報セキュリティ責任者は、効果的なガバナンス、リスク、コンプライアンスプログラムを構築し、これらの要件が共通のフレームワークに適用されていること、および自動化を利用して監査と管理を継続的に実施することを徹底する必要があります。」

戦略的アウトソーシング

は、最高情報セキュリティ責任者が複雑な業務を広範に管理する上で役立つ

ほとんどの最高情報セキュリティ責任者および彼らが所属する組織は、サイバー攻撃の検出、管理、防止においてアウトソーシングの価値を認識しています。

48%

主に社内のシステム、プロセス、スタッフを使用していると回答

30%

主にスペシャリストに外注していると回答

すべてを社内で管理している

18%

すべてを外注している

4%

現実には、ほとんどのITチームやサイバーセキュリティチームがすべてに精通しているとは限りません。アウトソーシングは、特に、継続的なモニタリング、深い専門知識、または社内の能力を超える大規模な対応が求められる分野において、重大なギャップを補うのに役立ちます。

外部パートナーが真の価値を提供できる例としては、サードパーティによるドメイン登録の検出と対応があります。新しいドメインは絶えず、そして比較的簡単に登録されるため、社内のチームだけで対応し続けることはほぼ不可能です。登録数の急増は、現実世界の出来事、製品の発売、公式発表などに反応して発生することが多く、こうしたパターンを追跡することで、従来のブランドモニタリングでは検出できなかった、新たな脅威や市場のシグナルを把握することができます。経験豊富なベンダーは、自動化されたモニタリング機能を提供し、大規模なスキャンを実施して、単なる潜在的な侵害だけでなく、より広範なビジネス・インテリジェンスに役立つ傾向を特定することができます。

しかし、自動モニタリングはほんの出発点に過ぎません。結果の解釈や、ドメインの防御的登録や削除の開始などの意思決定を誘導するには、人間の専門家が不可欠です。すべての組織が、ドメインの活動やその周辺状況について深い見識を持つスタッフを擁しているわけではありません。そのため、最新動向を常に把握しているパートナーを持つことで、重要な洞察と俊敏性を得ることができます。

> 「経験豊富なパートナーは、さまざまなサイバーセキュリティリスクの進化に対応しながら、顧客を全面的にサポートできます。今の傾向が、この先数ヶ月も続くとは限りません。何か新しいことが起こるかもしれません。その前に、必ず先手を打っておく必要があるのです。」

当社エキスパートの更なる見解

シンプル化を実現する提携：ドメインとDNSセキュリティを一元管理

ドメインおよびDNSセキュリティのアウトソーシングパートナーとの提携を検討する場合、組織が属する業界、デジタル資産ポートフォリオの構造、予算、リスク許容度に応じて戦略を立てることが重要だ、と ニーナは述べています。

そのためには、適切なプロバイダーを1社だけ選択することが重要です。複数の窓口があるとリスクが生じる可能性があるからです。 組織は、何か問題が発生した場合に、誰に連絡すべきかを明確にし、特に緊迫した状況では何社ものプロバイダーに連絡することにならないよう、戦略を合理化する必要があります。

また、信頼関係を構築し、社内と同じアプローチをプロバイダーも採用することを確信できるという側面もあります。

「業界の進化と新たな脅威の出現に話を戻すと、企業はその戦略を絶えず見直さなければなりません。なぜなら、ドメインや商標のポートフォリオが変化しない、まったく変化のないビジネスなど存在しないからです。

「同時に、企業は業界の動きにも遅れを取らないよう努めなければなりません。この点でも、信頼できるプロバイダーが大きな力になってくれます。」

多層的でコンプライアンスに準拠したセキュリティプログラムとは？

CSCは、ドメインセキュリティエコシステムにおける企業を支援する上で、最適な立場にあります。 これは、ドメインを含むさまざまなレイヤーに複数のセキュリティ対策を採用した、多層セキュリティというサイバーセキュリティアプローチを採用しているためです。 当社は、DDoS攻撃、ドメインスプーフィング、オンラインブランド乱用、フィッシングなどの脅威からお客様を保護します。

「ドメインセキュリティがなければ、セキュリティ体制は不完全です」と イハブは説明しています。 「モニタリングは重要ですが、それだけでは十分な対策にはなりません。 グローバルな権利執行メカニズムがなければ、企業に問題があることを通知するだけにとどまり、その問題を軽減する能力はありません。

ドメインが侵害されると、犯罪者はウェブサイト訪問者をフィッシングサイトにリダイレクトしたり、ブランドを偽って偽造品を販売したり、ウェブサイトやビジネスに不可欠な業務を停止させたりして、顧客の信頼や企業の評判を損なう可能性があります。

マーク ・フレッグは、ドメインとDNSが企業のオンラインプレゼンスの基盤を形成している点を強調しています。 「あなたの組織をトランプでできた家だと考えてみてください。 一番下の段は、あなたのドメインとDNSを表しており、オンラインでのあらゆる活動を支えています。 もし私がその一番下のカードの段を抜き取ったら、その上に築き上げたものはすべて崩れてしまいます。 あなたのウェブサイト、Eメール、そして音声IPを使用している場合は電話も使用できなくなります。 最高情報セキュリティ責任者は、そのような事態が発生した場合の「プランBは何か？」ということをあらかじめ考えておく必要があります。

つまり、企業はドメインセキュリティを、セキュリティ戦略全体の不可欠かつ基本的な要素として扱う必要があります。なぜなら、その部分が機能しなくなると、構造全体が危険にさらされるからです。

結論

最高情報セキュリティ責任者（CISO）は、組織のデータを安全に保ち、ますます複雑化する規制を遵守するという、ビジネスにおいて最も困難な職務の1つを担っています。サイバー脅威は、ドメインやDNS攻撃の分野を含め、その量と高度化が進んでいます。

AIはセキュリティ分野において貴重な用途がありますが、適切な保護対策が不十分な組織に甚大な被害をもたらす、新しい高度な手法の出現も招いています。

こうした課題があるにもかかわらず、当社が最初に公表した「最高情報セキュリティ責任者の展望」では、ほとんどの最高情報セキュリティ責任者のITセキュリティ予算は、前年比で緩やかな増加にとどまっていることが明らかになりました。これは、今日の組織にとって最も重大な脅威が実際にどこにあるかという点について、経営幹部層の間で理解の差があることを示しているかも知れません。

スタッフやパートナーがガバナンスプログラムを一貫して遵守していることを確認することが特に重要だとニーナは指摘します。

「チームの中で1人でも間違ったEメールを送信して、間違った情報を提供してしまう人がいれば、その影響は広範囲に及びます。これと同じことは、パートナーにも当てはまります」とニーナは言います。「1人のパートナーが何かミスを犯すだけで、非常に大きな問題につながる可能性があります。」

急速に変化する脅威環境において俊敏性を維持することは、ドメインやデジタルインフラストラクチャに関連するリスクの進化に関しては特に重要です。

このような背景から、最高情報セキュリティ責任者には次のことをお勧めします：

- 適切なツール、プロセス、スキル知識を適切に組み合わせた、よく構造化された多層的なセキュリティ戦略を採用する
- ユーザーモニタリング、従業員教育、サプライヤーのデータセキュリティ対策に特に重点を置いたGRCプログラムを確立する
- 社内チームの負担を軽減し、全体的な回復力を強化することができる、信頼でき、先見性のあるプロバイダーと提携する。

お客様の組織がドメイン管理とサイバーセキュリティにおいて常に一歩先を行くためのCSCのサポートについては、cscdbs.com/jp をご覧ください。

「なぜパスワードを頻繁に変更しなければならないかには理由があります。パスワードが長く使われているほど、誰かがそれを解読する可能性が高くなるからです」とマーク・フレッグは結論付けています。「これは、セキュリティ侵害や乗っ取り、偽のウェブサイトについても同様です。世に出回っている期間が長いほど、影響も大きくなります。管理は簡単なことではありませんが、常に先手を打つ必要があります。」

アンケート回答者の**概要**

業界セグメント

- 19% 金融機関
- 18% 医療・保険
- 17% 小売業界・消費財
- 16% テクノロジー、メディア、通信
- 11% 工業製品、エネルギー、公共サービス
- 20% その他すべて

回答者の役職

- 最高情報セキュリティ責任者 60%
- 最高情報責任者 13%
- シニアサイバーセキュリティディレクター、サイバーセキュリティ責任者 11%
- 最高技術責任者 8%
- IT責任者（または同等） 8%

企業本社（地域別）

33%
欧州

33%
北米

33%
アジア太平洋

お気軽にお問合せください

1 800 927 9800 | cscdbs.com/jp

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。

DBS09162025