KnowBe4

サイバー保険とセキュリティ: 高まる脅威への対応

Cyber Insurance and Security: Meeting the Rising Threat

サイバー保険とセキュリティ:
高まる脅威への対応

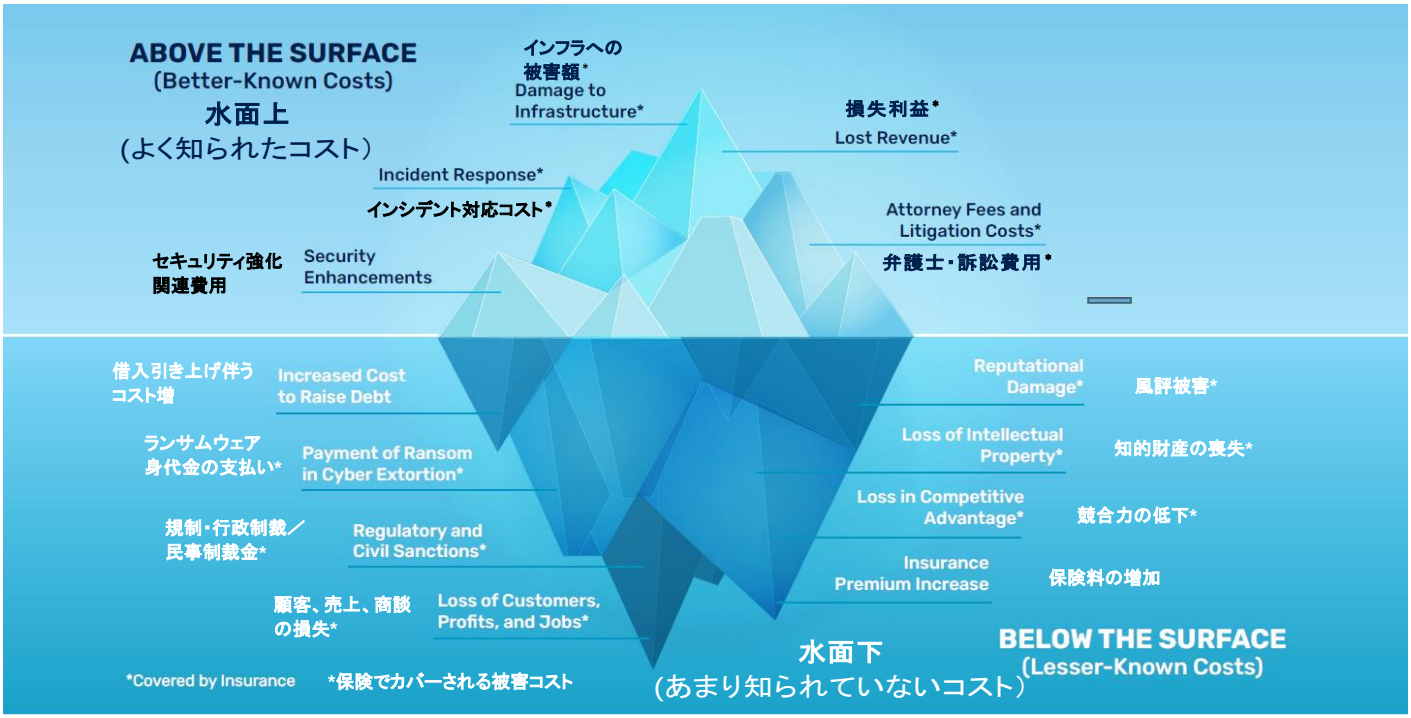
目次

デジタルシステムへの依存度が増す現代のエコシステムでは、ITインフラに内在する中断や侵入のリスクを無視することは、企業規模を問わず深刻な損害を招く可能性があります。場合によっては、事業の継続が困難となり、企業存続の危機に直面することさえあります。こうしたサイバーリスクを適切に管理するためのセキュリティ対策の強化や、対策が失敗した場合に備えた保険の重要性を軽視することは、もはや許される選択肢ではありません。

サイバー攻撃の被害コスト

サイバー攻撃の影響と被害コストは、目に見えやすいサービス中断やデータ流出にとどまらず、莫大なものになる可能性があります。業務が復旧した後でも、民事訴訟、規制当局からの罰金、風評被害や競争力低下の修復費用などが発生する可能性があり、被害コストは膨れ上がる一方です。

サイバー攻撃の影響[1]



2024 IBM Cost of a Data Breach[2]レポートによると、データ侵害の平均コストは488万ドルで、2023年の445万ドルから増加し、2018年の386万ドルから増加しました。平均額を上回ったのは、米国（936万ドル）、中東（875万ドル）、ベネルクス（590万ドル）、ドイツ（531万ドル）の4つです。

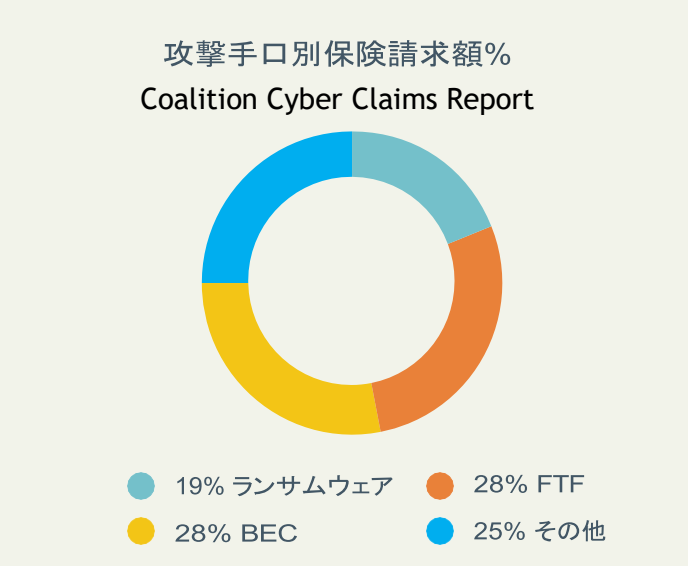
2024年の報告書では、5万ドル以上の罰金を支払う組織の数が22.7%増加し、10万ドル以上の罰金を支払う組織の数が19.5%増加しました。

1 "Cyber Insurance: What You Need to Consider Before Purchasing a Policy," Chase, J.P. Morgan リンク
2 IBM Cost of a Data Breach Report 2024 リンク

保険業界が見たサイバーリスクの現状

サイバー保険とセキュリティの大手企業であるCoalitionが発行した2024年度のCyber Claims Report[3]は、2023年に米国でFBIが受けたサイバー犯罪の保険請求は88万件を超え、報告被害額は125億ドルに達し、前年比13%増であった[4]と報告しています。

また、同社の資金移動詐欺（Funds Transfer Fraud: FTF）の保険金請求は2023年に24%増加し、平均損失額は278,000ドルを超えました。進化し続けるフィッシングメールは、ますます検知が難しくなっています。脅威者はAIを利用して、より迅速に情報を解析し、より的確にコミュニケーションを取り、特定の企業を標的とし、フィッシングキャンペーンをより効果的に展開していると考えられます。



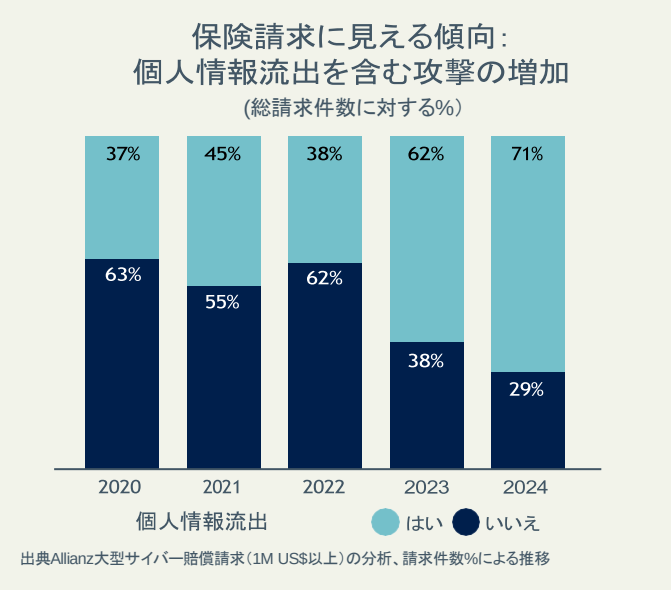
Allianz Commercial社は、全世界の3069社の企業を対象に、各業界が直面する最も重要なリスクについて調査を行い、2024年版報告書[5]を作成しました。回答企業が報告したリスクのカテゴリーで最も高かったのはサイバーインシデントで、ITネットワークやサービスの中断、マルウェア／ランサムウェア、データ侵害、罰金、罰則を含んでいました。サイバーリスクは36%で、サプライチェーンの混乱、規制や経済の変化、自然災害、政情不安を大きく上回りました。最も懸念しているリスク要因としては、59%がデータ漏洩を挙げています。

同社がこの期間の保険金請求を分析した結果、同社の懸念について根拠を裏付けています。2024年の報告書では、サイバー犯罪による損害賠償請求は17%増加しましたが、2023年ではわずか1%増加しただけでした。100万ユーロを超える大規模なサイバー犯罪による損害賠償請求(110万ドル)が、2024年上半期に14%増加し、大型損害賠償請求の72%は米国でした。

主な要因は、ランサムウェア攻撃の増加です（2024年上半期の大規模なサイバー損害賠償請求額の58%をランサムウェアが占めています）。機密性の高い個人情報の流出は攻撃の範囲を拡大し、多くの場合、被害コストに規制違反による罰金が加わります。また、身代金要求が増加したのに加えて、データの販売から追加収入を得ることができるため、個人情報の流出は攻撃者にとってますます大きな標的となっています。

データ流出の増加により、個人情報の侵害を主張する集団訴訟も急増しました。これは特に米国で顕著で、包括的なデータプライバシー（個人情報保護）法を制定した州は2023年に入ってから5州から13州に増加しました。アジア太平洋地域でもデータプライバシー（個人情報保護）法は大きな進展が見られ、日本、韓国、インド、中国で、個人情報流出に対する訴訟への道が開かれています。

3 Coalition 2024 Cyber Claims Report
4 Federal Bureau of Investigation, 2023 Internet Crime Report
5 Cyber security resilience 2024 webinar, Alliance Commercial リンク



アリアンツの報告書によると、米国では個人情報のデータ侵害による集団訴訟が急増しており、米国の集団訴訟の中で最も急成長している分野の1つとなっています。2023年に米国で提起されたデータプライバシー（個人情報保護）関連の集団訴訟は1,300件以上。これは2022年の2倍以上、2021年の4倍です。報告書では「データプライバシー（個人情報保護）をめぐる複雑な規制と法的状況が集団訴訟の原因を作り出している」と指摘しています。個人情報のデータ保護の権利に対する意識が高まり、第三者による訴訟資金調達が消費者により優しい訴訟環境に寄与しているため、欧州でも同様の上昇が見られる可能性があります。

インシデント被害コスト

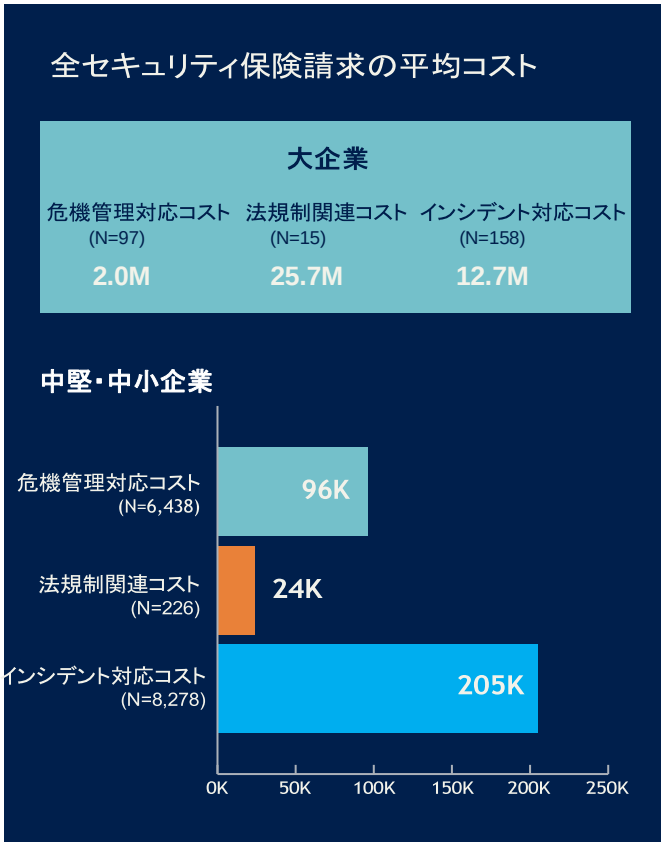
NetDiligence Cyber Claims Study Report 2024[6]では、2019年から2023年の5年間に発生したインシデントに対する1万件以上のサイバー保険請求を分析しています。保険請求の98%（総額19億ドル）は、年間売上高20億ドル未満の中堅・中小企業（SME）からでした。年商20億ドル以上の大企業からの保険請求が2%（合計20億ドル）。サイバー保険請求額は1,000ドル未満から5億ドル超まででした。データ流出で公開されたレコードの数は1件から1億4,000万件超でした。

NetDiligence のレポートでは、サイバーインシデントの被害コストを次の3つのカテゴリーに分けて追跡し、調査しています。

- 危機管理コスト: 初期対応からフォレンジック（被害状況調査、原因究明）、内部・外部への通知、広報、再発防止策の実施など
- 法規制関連コスト: 訴訟弁護、訴訟和解、規制措置弁護、規制罰金など
- インシデント対応コスト: システム復旧をはじめとするインシデント対応に関連するあらゆる種類のコスト／経費の総計

大企業で発生したインシデント対応の平均コストは、中堅・中小企業で発生したインシデント対応の平均コストの62倍以上でした（1,270万ドル対 20万5,000ドル）。

平均額が小さいにもかかわらず、中堅・中小企業では大きなインシデント対応コストを費やしており、おそらく組織への影響も大きくなっています。中堅・中小企業による保険請求には、100万ドルを超える保険請求が327件あり、1億ドルを超えるも2件含まれています。



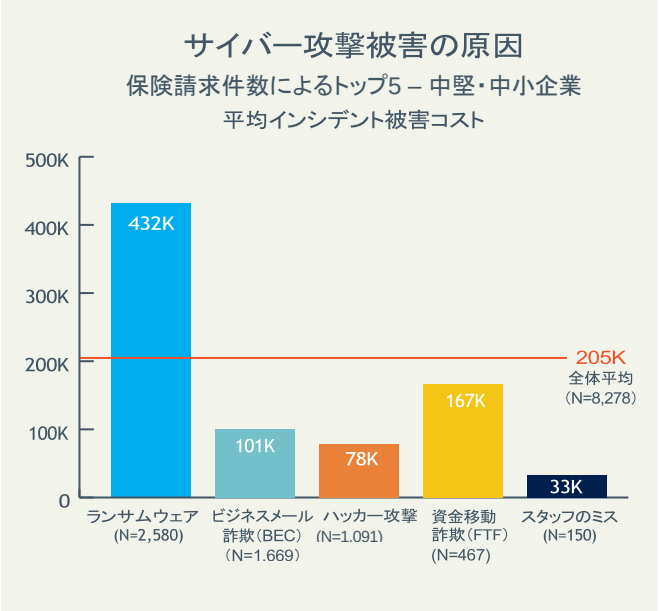
6 NetDiligence Cyber Claims Study Report 2024 リンク

危機管理コスト

すべての組織規模において、危機管理コストは10万ドル未満から2,600万ドル近くまで幅がありました。中堅・中小企業では、危機管理コストがインシデントコスト全体の62%を占め、1インシデントあたりの平均コストは14万6,000ドルでした。大企業でも、クライシス・サービス費用はインシデントコスト全体の62%を占め、1インシデントあたり平均190万ドルでした。これらの費用の大部分（60%以上）は、フォレンジック（被害状況調査、原因究明）と内部・外部への通知に対するものでした。

サイバー攻撃被害の原因

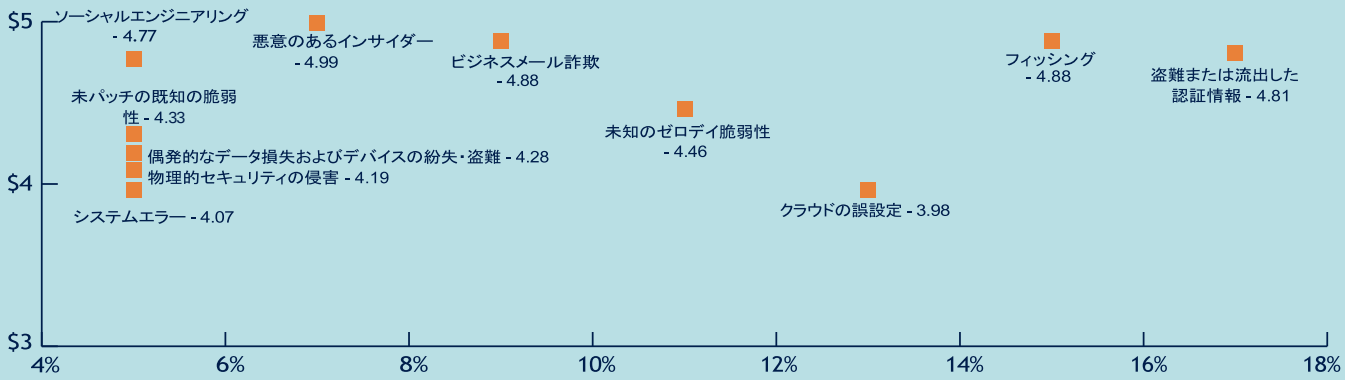
NetDiligence レポートの5年間で、中堅・中小企業によるサイバー保険請求の97%は、ハッキング、ランサムウェア、ソーシャルエンジニアリング、ビジネスメール詐欺（BEC）、フィッシング、デバイス盗難/金銭盗難、銀行/ACH（自動決済機関）決済詐欺、DDoS（分散型サービス拒否）攻撃といった犯罪行為によるものでした。同時期の大企業によるサイバー保険請求でも、このような犯罪行為が大半を占め、86%でした。



ランサムウェアとビジネスメール詐欺（BEC）が攻撃被害の2大原因であり、2019年から2023年の5年間で$1,000を超える請求の53%を占めています。また、同報告書によると、ランサムウェアによる被害額は、跳びぬけて多く、要求額は8000万ドルで支払われた身代金は5000万ドルを超えています。また、1,000万ドル以上の身代金が支払われたランサムウェア攻撃が15件発生しています。

ランサムウェアは4年連続で中小企業の財務上の脅威のトップであり続け、年々増加し続けています。2024年におけるランサムウェアの平均被害額は43万2,000ドルで、昨年の報告書の33万4,000ドルから増加しています。

また、IBM Cost of a Data Breach レポートはフィッシング、盗難または流出した認証情報、ビジネスメール詐欺（BEC）を初期攻撃ベクトルおよび最も被害の大きい攻撃の上位に挙げています。



7 “Cost of a Data Breach 2024,” IBM. リンク

IBMの数字によると、ソーシャルエンジニアリングとフィッシングが、データ侵害を達成するために使用される最大の攻撃手法（44%）となっています。ソーシャルエンジニアリング以外の人的リスク要因として、悪意のあるインサイダー（7%）、物理的セキュリティの侵害（6%）、偶発的なデータ損失やデバイスの紛失・盗難（6%）、クラウドの誤設定（12%）を加えると、人的リスクはデータ侵害の原因全体の75%を占めています。

最も効果的な保険会社は攻撃前からの予防のための支援を提供します

保険会社は、顧客と利害を共有しています。サイバー攻撃によるリスクを低減し、被害を軽減することは、保険会社と顧客企業の双方に利益がもたらされます。ここに必要なのは、攻撃が発生する前に攻撃を遮断する予防のための共同努力と注力です。保険会社と顧客企業の双方の効果的なパートナーシップを通して、顧客企業はサイバーリスクを確実に軽減し、安定と財務の健全性を享受することができます。また、同時に、保険料の引き下げを可能にし、より良い補償を利用できるようになります。効果的なパートナーシップのために必要な最低限のフレームワークには、次の3つのポイントが含まれます。

対処すべき脅威へ正しく選択する[8]

70-90%
の攻撃は
ソーシャルエンジニアリング
から発生する

33%
の攻撃には
未パッチのソフトウェア／
ファームウェア
が関与する

30%
の攻撃には
脆弱／不正な
ログイン
が関与する

79% | はソーシャルエンジニアリングよって盗まれた不正なログイン

ソーシャルエンジニアリングのリスクを軽減する

保険会社とともに、少なくとも、次の対策を確認する必要があります。

- フィッシングに強い多要素認証（MFA）を使用していますか？
  中間者攻撃（MitM攻撃）によってスプーフィングされる可能性がある場合、MFAは脆弱です。MFAが入力すべきコードや承認のためのプロンプトを送信する場合も、同様に脆弱です。一要素認証（1FA）は、許可すべきではありません。
- ログインには、フィッシングに強いMFAを使用していますか？
- フィッシングに強いMFAが可能でない場合、どのようなMFAを使用していますか？

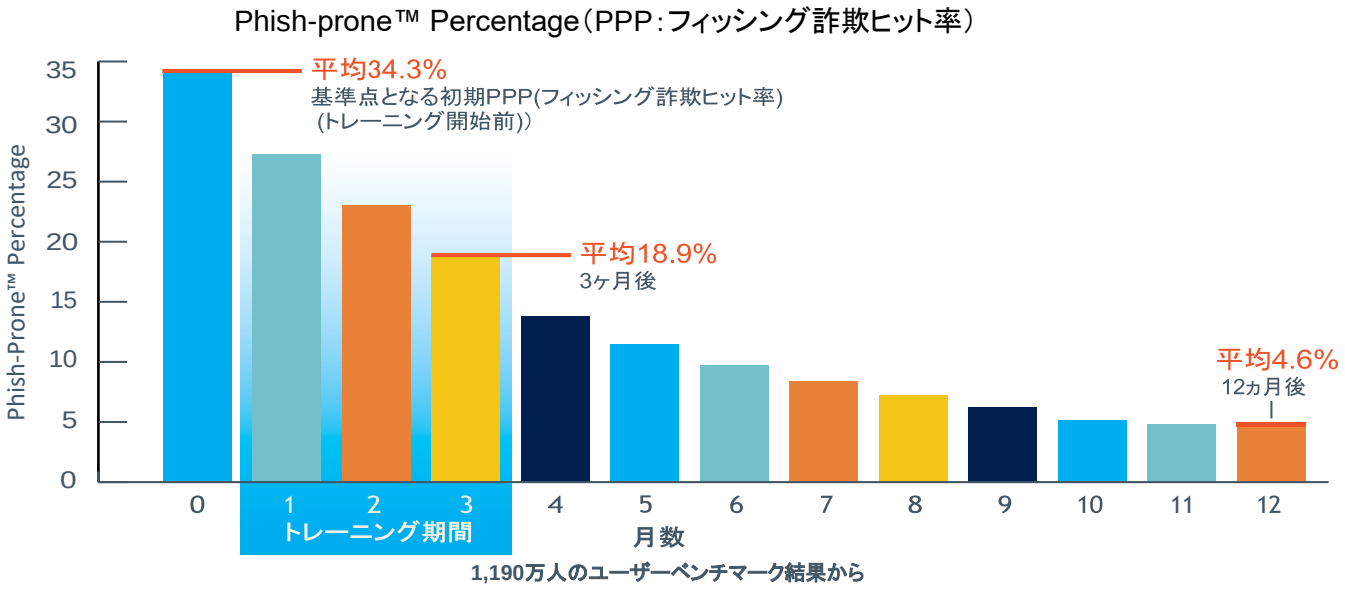
8　ロジャー・グライムス KnowBe4プレゼンテーション

- MFAが可能でない場合は、Webサイトやサービスごとに、異なる、推測不可能／クラッキング不可能なパスワードを要求していますか？（12文字のランダムパスワードは、既知の推測／クラッキング攻撃をすべて防御する）。
- すべてのパスワードにパスワードマネージャーを使用することを検討していますか？
  パスワードマネージャーは、サイトやサービスごとに強力でユニークなパスワードを作成し、簡単に使用できるようにします。
- パスワードマネージャーを使用する場合、パスワードマネージャーはMFAおよび/または長いパスワードで保護されていますか？
- すべてのパスワードは、少なくとも年1回変更していますか？
- 的確な脆弱性評価を実施していますか？
- 模擬フィッシング演習を含む効果的で頻繁なセキュリティ意識向上トレーニングを導入していますか？

保険会社は、セキュリティ意識向上トレーニングの実施について、初期アセスメントで「はい／いいえ」のチェックボックスで確認する必要があります。これは、顧客企業や組織にとって、セキュリティ意識やセキュリティ教育の欠如は極めて危険なものであるにもかかわらず、最も認識されていないセキュリティ上のリスクのひとつであるためです。また、保険会社にとっては、セキュリティ意識向上トレーニングは保険会社最大の利益を生み出す可能性がある領域でもあります。

KnowBe4では、この人的なセキュリティリスクを判定するために、フィッシングセキュリティテスト（PST）を提供しています。PSTは、フィッシングリンクを埋め込んだフィッシングメールを送信して、どれくらいの顧客組織の従業員がこのフィッシングメールに騙されてクリックするかをテストするものです。KnowBe4では、お客様のニーズに合わせて、複数の異なるタイプのPSTを提供し、Phish-prone™ Percentage（PPP：フィッシング詐欺ヒット率）を集計し、従業員一人ひとりがどれくらいフィッシングやソーシャルエンジニアリング攻撃の被害を受けやすいかを明確にしています。KnowBe4のセキュリティ意識向上トレーニングを受ける前の初期テストのPPPが30～35%になることも珍しくありません。つまり、およそ3人に1人の従業員が、ハッカーや詐欺師のメールに記載されたリンクをクリックしてしまう可能性があるということです。

これらの割合は、1年以上継続的にサイバーセキュリティに関するセキュリティ意識向上トレーニングと模擬フィッシング演習テストを受けると劇的に低下します。2024年KnowBe4フィッシングベンチマーキングレポートの結果によると、すべての業種と規模において、ベースライン・テストから1年以上の継続的なトレーニングとテストを実施することで、「フィッシングにかかりやすい」従業員の平均数が34.3%から4.6%に減少しました。



1,190万人のユーザーベンチマーク結果から

協力し合う

保険会社、顧客企業、サイバーセキュリティ・ベンダーは協力し合うことで、より強力で包括的なサイバーセキュリティ保険を構築することができます。保険会社は、KnowBe4のPhish-prone™ Percentage（PPP：フィッシング詐欺ヒット率）のようなリスクスコア分析によって証明される組織内の強力なセキュリティ対策を探究することができます。そして、保険会社は、このような実践を実証した組織には（保険料の控除など）金銭的なインセンティブを与えることができます。

まとめ

急速に進化するサイバー脅威の状況は、世界中のあらゆる組織にかつてない課題を突きつけています。デジタルエコシステムがますます複雑になるにつれ、壊滅的なサイバー攻撃の可能性は飛躍的に高まっています。不慮のデータ流出、ランサムウェア攻撃などのサイバーインシデントによって発生する途方もない被害コストは、サイバーセキュリティへの包括的なアプローチの必要性に加えて、より具体的には、人的リスク管理の重要性を明確に示すものです。

＜本稿の要点＞

- サイバー攻撃による財務上の影響は深刻化しており、2024年には平均被害コストが488万ドルに達し、世界各国で大幅に高額になっています。
- サイバーインシデントは、サプライチェーンの混乱や自然災害といった従来の懸念事項を凌駕し、今や世界的な企業のトップリスクと考えられています。
- ソーシャルエンジニアリングとフィッシングは、依然として最も一般的な攻撃手法であり、成功したデータ侵害の原因の大部分を占めています。
- 法律や規制の状況はより複雑になっており、データプライバシー（個人情報保護）法の増加により集団訴訟が急増しています。
- 中堅・中小企業は特に脆弱であり、サイバーインシデントによって壊滅的な損失を被る可能性があります。
- サイバーセキュリティの弱点は依然として人的要因であり、データ漏洩の75%は人的リスクに起因しています。

保険会社は、セキュリティ意識向上トレーニングの実施について、初期アセスメントで「はい／いいえ」のチェンジボックスで確認することがあります。これは、顧客企業や組織にとって、セキュリティ意識やセキュリティ教育の欠如は極めて危険なものであるにもかかわらず最も認識されていないセキュリティ上のリスクのひとつであるためです。また、保険会社にとってみれば、セキュリティ意識向上トレーニングは保険会社最大の利益を生み出す可能性がある領域でもあります。

これらの課題に対処するためには、多面的なアプローチが必要です。

- フィッシングに強い多要素認証やソフトウェアの定期的なアップデートなど、強固なサイバーセキュリティ対策に投資する。
- 全従業員に対する包括的かつ継続的なセキュリティ意識向上トレーニングプログラムを実施します。
- 定期的な脆弱性評価と侵入テストを実施する。
- プロアクティブなリスク管理サービスを提供するサイバー保険プロバイダーと連携・連帯する。
- 進化するサイバー脅威に関する情報を常に入手し、それに応じてセキュリティ戦略へ適応させる。
- 攻撃発生時の被害を最小限に抑えるため、インシデント対応計画を策定し、定期的にテストする。

結論として、サイバー脅威の状況は、企業、保険会社、サイバーセキュリティの専門家による一歩先を見据えたプロアクティブで協力的なアプローチを必要としています。保険を通じて、サイバー攻撃への予防、教育、リスク対応に注力することで、企業は増加するサイバー脅威に立ち向かい、進展するデジタル化の世界で自社の資産、評判、顧客を保護することができます。

KnowBe4がサイバー保険料の低減に役立つ

KnowBe4のプラットフォームがサイバー保険料の低減に役立つことは、当社のお客様が以下のように証明しています。

「KnowBe4セキュリティ意識向上トレーニング（KSAT）を利用していることを保険会社に示すことができ、その結果、サイバー保険の保険料が20%安くなりました。

– ITセキュリティアナリスト、顧客A

「サイバー保険の入札には競合がありました。入札の多くは、過去に私たちをカバーすることを拒否した会社からのものでしたが、KnowBe4と協力しているため、今では保険料が下がりました」。

– セキュリティアナリスト、カスタマーF

「KnowBe4セキュリティ意識向上トレーニング（KSAT）を利用していますので、先月、初めてサイバー保険に加入しました。保険会社は、以前は我々を見向きもしなかったのですが。」

– アソシエイトディレクター、サイバーセキュリティ、カスタマーK

その他の関連情報

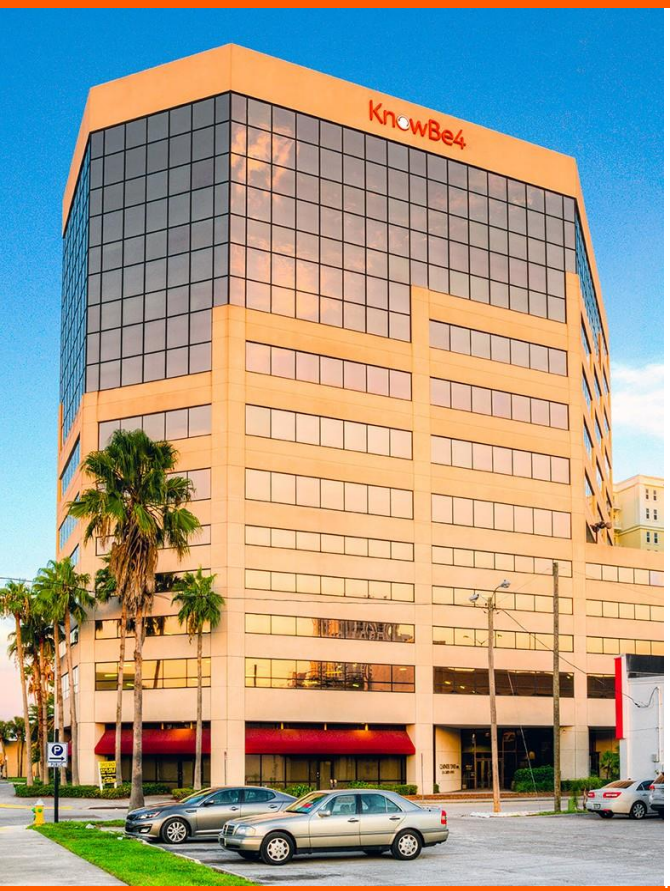
フィッシングセキュリティテスト
あなたの企業や組織の従業員の何パーセントがフィッシング攻撃に引っかかるかをスコア化することができます。.

セキュリティプログラムビルダー
あなたの企業や組織のためにカスタマイズされたセキュリティ意識向上プログラムの作成を自動化します。

Phish Alertボタン
あなたの企業や組織の従業員がフィッシング攻撃の報告をワンクリックで行うことができます。

無償Email Exposure Checkツール
あなたの企業や組織の従業員のメールアドレスが、どれくらいインターネット上で公開されているかをチェックできます。

無償なりすましドメインテスト
ハッカーがあなたの企業や組織のドメインのメールアドレスを偽装できるかをチェックできます。



＜KnowBe4について＞

KnowBe4は、セキュリティ意識向上トレーニングとフィッシングシミュレーション・分析を組み合わせた世界最大の統合型プラットフォームです。セキュリティの人的要素への抜本的な対策の欠如に気づき、KnowBe4は「人」を狙うセキュリティ脅威から個人、組織、団体を防御することを支援するため設立されました。

KnowBe4プログラムは、偽装攻撃によるベースラインテスティング、クラウドベースのインタラクティブなトレーニング、継続的なアセスメントを組み合わせた統合型のアプローチです。ここには、フィッシング、ビッシング、スミッシングといった多彩な偽装攻撃を通しての本番さながらのフィッシング体験とトレーニングがあります。セキュリティ第一のマインドセットを形成し、組織全体のセキュリティカルチャーを醸成します。

金融機関、製造業、エネルギー産業、医療機関、官公庁、生損保などで、7万社を超える企業や団体がKnowBe4を採用して、防御の最終ラインとして「人」による防御壁を構築して、日々求められるセキュリティ上の的確な意志決定を可能にしています。

詳しくは、www.KnowBe4.jpをアクセスしてください。

KnowBe4 Human error. Conquered.

KnowBe4 Japan 合同会社　〒100-6510 東京都千代田区丸の内1－5－1
新丸の内ビルディング10F EGG 内
Tel: 03-4586-4540 | www.KnowBe4.com／www.KnowBe4.jp |