



KnowBe4

フィッシング ベンチマーキング レポート

| アジア地域 2025年度版



ヒューマンリスクを明確にして フィッシングメールのクリック率を低減

ヒューマンリスク管理 (HRM) を効果的に実施するには、
フィッシングのリスクを減らすことが最も重要です。

フィッシング攻撃が成功する確率は、リンクのクリックなどの特定の行動が実行されるかどうかにかかっています。フィッシングメールが技術的な防御をすり抜けたとしても、受信した社員が、そのメールを報告・削除したり、それに反応しなければ攻撃は成功しないからです。

AI搭載のフィッシング対策製品を導入して技術的な防御を強化しながら、ベストプラクティスに基づく最適なセキュリティ意識向上トレーニング (SAT) を実施することで、組織におけるフィッシングリスクを大幅に軽減することができます。

リスク軽減における効果的な戦略の第一歩は、まず自社のリスクプロファイルを理解し、業界や組織規模が同じような企業や、同じ地理的地域にある他の企業と比較して、自社がどのような位置づけにあるかを分析することです。次に、フィッシングメールと接触する可能性のある人物を特定し、組織がフィッシング攻撃に対して実際にどの程度脆弱であるかを把握します。これらの情報を得ることで、個々にカスタマイズされたトレーニングプログラムやリアルタイムコーチングなど、個人に合わせたセキュリティ対策を適切なタイミングで講じることができます。

KnowBe4の業界別フィッシングベンチマーキングレポートは、この戦略の最初のステップを提供します。今年度のレポートでは、62,460の組織に所属する14,508,441人のユーザーを対象に、合計67,718,305件のフィッシングシミュレーションを3年間にわたり分析し、19の業界と7つの地理的地域にわたる組織の「Phish-prone™ Percentage (PPP: フィッシング詐欺ヒット率)」を算出しました。

本書では、アジアにおける主な調査報告をまとめてご紹介します。

PPP (フィッシング詐欺ヒット率) の算出方法

PPP は、組織内の従業員のうち、ソーシャルエンジニアリングやフィッシング攻撃の被害に遭う可能性のある従業員の割合です。これらは「フィッシングシミュレーションクリック率」と呼ばれることもあります。

フェーズ1

ベースラインベンチ
マーキング (トレーニング
開始前の事前テスト)

KnowBe4のトレーニングを実施する前に、最初の模擬フィッシングを送信します。これを使用して、リスクを特定し、組織のベースラインPPPを算出します。

フェーズ2

トレーニング開始後90日
までのベンチマーキング

従業員は、KnowBe4のセキュリティ意識向上トレーニングを受けます。別のシミュレーションが送信され、組織のPPPを再計算し、トレーニングプログラムの有効性を測定します。

フェーズ3

トレーニング開始1年後
からそれ以降の
ベンチマーキング

KnowBe4のセキュリティ意識向上トレーニングを12か月間実施した後、PPPを再計算し、トレーニングプログラムの効果をさらに定量的に評価します。

2025年度 グローバルフィッシングベンチマーク

地域別に見ると、南アメリカ (39.1%)、北アメリカ (37.1%)、およびオーストラリア・ニュージーランド (36.8%) でベースラインPPPが高くなっています。

オーストラリア・ニュージーランドに本社のある従業員1,000人以上の企業では、44.6%が模擬フィッシングのリンクをクリックしており、世界で最もフィッシング攻撃に脆弱であることがわかりました。最もリスクが低いのは、アジアと英国・アイルランドの従業員数1~249人の小規模組織で、これらの組織でリンクをクリックしたのは従業員の4分の1 (24.3%) でした。

すべての地域で平均改善率80%以上が達成されました。北アメリカが89.5%と最も高く、次は南アメリカの88.9%でした。

	組織の規模	フェーズ1—ベースライン			フェーズ2—90日後			フェーズ3—1年後		
		1-249人 従業員数	250-999人 従業員数	1,000人以上 従業員数	1-249人 従業員数	250-999人 従業員数	1,000人以上 従業員数	1-249人 従業員数	250-999人 従業員数	1,000人以上 従業員数
地域	北アメリカ	26%	31.1%	42%	21.1%	21.2%	18.5%	3.7%	3.9%	4.1%
		合計: 37.1%			合計: 19.6%			合計: 3.9%		
	アフリカ	27.9%	30.1%	35.8%	24.9%	28%	20%	2.2%	9.2%	5.1%
		合計: 34.9%			合計: 21.1			合計: 5.3		
	アジア	24.3%	27.6%	29%	18.9%	19.1%	17.6%	5.1%	4.5%	5.4%
		合計: 28.6%			合計: 17.9%			合計: 5.2%		
	オーストラリア・ ニュージーランド	25%	29.2%	44.6%	23.2%	23%	16.6%	3.9%	6.1%	4.7%
		合計: 36.8%			合計: 19.9%			合計: 4.9%		
	ヨーロッパ	24.9%	26.7%	34.9%	20.7%	21.6%	20.5%	3.9%	4.4%	5.3%
		合計: 32.5%			合計: 20.7%			合計: 5%		
	南アメリカ	30.2%	26.3%	42.8%	23.3%	23.1%	16.9%	3.4%	5.1%	4.5%
		合計: 39.1%			合計: 18.2%			合計: 4.5%		
	英国・アイルランド	24.3%	28.5%	36%	22.1%	22.1%	17.1%	4%	4.1%	5.3%
		合計: 32.9%			合計: 19%			合計: 4.8%		

アジア | By Caroline Soo and Bex Bailey

アジアの組織で、ベストプラクティスに基づく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に投資している組織は、クリック率が81.8%という驚異的な減少を実現しています。データ漏洩の割合やコストの高い地域では、これは喜ばしい傾向です。フォレスターの[2024 Breach Benchmarks By Region](#) (2024年地域別侵害ベンチマーク) レポートによると、アジア太平洋地域 (APAC) の組織が12か月間に経験したデータ侵害は平均3.5件でした (世界平均は2.8件)。また、その累積コストは、世界平均が270万米ドルであるのに対し、280万米ドルとなっています。

フィッシングからサイバー犯罪につながるが多いため、このリスクを減らすことが組織のセキュリティには非常に重要です。

セキュリティトレーニングを導入する前、アジアの企業では従業員の28.6%がフィッシングシミュレーションで使われるリンクをクリックしていました。このリスクは組織の規模に応じて増えており、世界的にも同様の傾向が見られます。従業員数1~249人の組織のリスクが24.3%と最も低く、250~999人の組織では27.6%、1,000人以上の組織では29%まで増加しました。

90日間のトレーニングを実施した後、このリスクは大幅に減少し、平均17.9%まで低下しました。この段階で最も改善が見られたのは大規模組織であり、従業員数1,000人以上の組織での平均クリック率は17.6%でした。トレーニング実施から1年後には、このリスクは平均5.4%まで下がっています。

業界別に見ると、最初のクリック率は保険会社が43.6%と、この地域で最も高く、地域平均を15%上回っています。その他のセクターでも銀行 (39.1%)、教育 (37.9%)、ホスピタリティ (36.7%)、非営利団体 (33%) などですべてリスクが高いことがわかりました。

なかでも、ホスピタリティ業界は最適なトレーニングを1年間実施した後クリック率が94.8%も減少し、最も顕著なリスクの削減を実現しています。その他のセクターでも、非営利団体 (88.5%)、教育 (82.8%)、銀行 (79.8%)、保険 (63.8%) などですべてリスクの減少を示しました。

アジア

PPP (フィッシング詐欺ヒット率)

組織の規模	フェーズ1ー ベースライン	フェーズ2ー 90日後	フェーズ3ー 1年後
1-249人	24.3%	18.9%	5.1%
250-999人	27.6%	19.1%	4.5%
1,000人以上	29.0%	17.6%	5.4%
全組織規模に おける平均PPP	28.6%	17.9%	5.2%

アジアにおけるヒューマンリスクに影響を与えるサイバー犯罪の傾向

アジアでは、デジタル化の計画が複雑になっています。世界経済フォーラムは、東南アジア諸国連合 (ASEAN) を「世界で最も急成長しているインターネット市場」と評し、そのデジタル経済の成長により、今後10年間で地域のGDPは1兆米ドル増えると推測しています。

トレーニングを1年間継続した結果、
最初の段階から平均78%低減され、
あらゆる企業規模の大半の業種で
PPP率が1桁台になりました

その他にも、中国や日本もまた大きなデジタルフットプリントを有しています。特に日本は、高度に接続されたインフラストラクチャーと先進的な技術環境を有し、そのセキュリティにますます力を注いでいます。例えば、新たに可決された能動的サイバー防御法案は、サイバー攻撃がエスカレートする前に阻止するための政府の権限を強化するものです。

急速なデジタルトランスフォーメーションと成熟したテクノロジーエコシステムが組み合わさることにより、地域全体で人々やその雇用者にさまざまな脅威をもたらしています。この地域全体のヒューマンリスクに影響を及ぼす要因を見ましょう。

サイバー犯罪の「中心地」

国連薬物・犯罪事務所 (UNODC) の[レポート](#)によると、東南アジアにおけるサイバー利用犯罪は激化の一途をたどっており、その被害の大部分はこの地域に拠点を置くサイバー犯罪組織に起因しています。UNODCは、これらの国々、特にメコン地域にある国を、多角化を目指す多国籍犯罪ネットワークの「重要な実験場」と見ており、「詐欺産業の中心地」と考えています。

サイバー犯罪者が世界規模での攻撃の拡大を図る中、特にアジアの人々やインフラは、新たな脅威に狙われる可能性があるでしょう。

サプライチェーンにおける急速なデジタル化

PriceWaterhouseCoopers (PWC) は、APACの63%の組織がサードパーティサプライヤーに過度に依存しており、それが関連する脅威によるリスクエクスポージャーを増大していると考えていると[発表しました](#)。

これは、デジタルトランスフォーメーションが急速かつ不均等なペースで進んでいることや、一部の国やセクターにおいてインフラが老朽化したり、また新たに導入されたりすることによってさらに増幅しています。PWCのレポートでは、サイバーセキュリティの上位の懸念事項が、ソフトウェアセキュリティ、ゼロデイ脆弱性の悪用、サプライヤー自身による侵害など、サードパーティーのエコシステムに直接関連していることが確認されています。

生成AIがフィッシング詐欺のローカライズを可能に

生成AIが普及する以前は、世界的なフィッシング詐欺の多くは英語で実施されてきました。USENIXが発表した[調査](#)によると、英語を母国語としない場合、英語で書かれたEメールを不審に思い、メールに書かれた指示を無視する傾向が高い

ことがわかっています。

これまでは、現地の言語でフィッシングメールを作成したり、翻訳したりするには高い専門知識が必要であったため、世界的な攻撃を仕掛けることは困難でした。しかし、世界の他の地域と同様に、大規模な言語モデル (LLM) により、現地の言語によるフィッシングメールの迅速かつ高精度な作成が可能になり、AIを応用した攻撃のパーソナライゼーションや自動化が進んでいます。

まとめ (確認ポイント)

- ▶ アジアはサイバー犯罪の発生地になっており、個人や組織が攻撃の実験場を形成している
- ▶ APAC地域の組織は、世界平均と比較してより頻繁に攻撃を受けており、フィッシングメールによる最初の攻撃を阻止する必要性が高まっていることを示している
- ▶ 生成AIはフィッシングのリスクを増大している。現地の言語で人々を標的にしやすくなり、これらの脅威と連携する傾向が高まっている
- ▶ サイバーセキュリティトレーニングの導入により、組織はフィッシングのクリック率を81.8%削減することができ、ベストプラクティスに基づく最適なプログラムがもたらす価値を実証している

詳しくは以下をご覧ください

www.KnowBe4.com/ja →

KnowBe4について

KnowBe4は、全従業員が、毎日セキュリティに関してより賢明な判断を下せるようサポートします。セキュリティカルチャーを強化することで人に関わるリスクを低減するKnowBe4の製品は、世界の7万社を超える組織から支持を集めています。KnowBe4は「ヒューマンリスク管理」を念頭に置き、AIを搭載した包括的な「ベスト・オブ・スイート」プラットフォームを提供しており、最新のサイバーセキュリティ脅威に対するユーザーの行動強化に役立つ適応型の防御層を構築します。HRM+プラットフォームには、意識向上やコンプライアンスにおけるトレーニング、クラウドメールセキュリティ、リアルタイムコーチング、クラウドソース型アンチフィッシング、AIディフェンスエージェントなどのモジュールが含まれています。KnowBe4は他に類を見ないグローバルなセキュリティプラットフォームであり、パーソナライズされた適切なサイバーセキュリティ保護コンテンツ、ツール、テクニックを活用し、最大の攻撃対象である「従業員」を組織最大の資産へと変えていきます。

詳細については、www.KnowBe4.com/jaを参照してください。

KnowBe4

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

03-4586-4540 | www.KnowBe4.com/ja | info@KnowBe4.jp

本書に記載されている他社の製品および会社名は、各社の商標または登録商標です。