

業界別フィッシング ベンチマーキングレポート

アジア地域 2026年度版



アジア地域 2026年度版

AIがもたらすヒューマンリスクにどう向き合うか

フィッシング詐欺のリスクを抑えることは、
デジタルワークフォースと言われる「AIエージェントと人」の安全を確保する上で極めて重要です。

サイバー攻撃が成功するかどうかは、リンクのクリックや添付ファイルのダウンロード、認証情報の入力といった個人の行動に大きく依存しています。フィッシングメールが技術的な防御をすり抜けて届いてしまったとしても、受け取った側に「報告する」「削除する」「単に無視する」といった直感的な判断があれば攻撃を防ぐことができるからです。

大前提として、組織がAIを活用したメールセキュリティ施策を講じ、技術的な障壁を強化し続けていくことは不可欠です。しかしその上で、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(SAT)の実施が、リスクを大幅に軽減するということを本レポートのデータは証明しています。

現在の組織には、人だけでなくAIエージェントも業務に導入されており、従来の技術的対策では想定されていなかったような形で攻撃対象が広がっています。そのような環境の中で、SATは、デジタルワークフォースに対するセキュリティを最も効果的な手段で強化すると同時に、人間とAIが共存する労働環境が生み出すリスクを管理するための基盤として、セキュリティカルチャーの醸成と組織的な警戒体制の構築をサポートします。

ベンチマーキング:レジリエンス向上のための第一歩

効果的なリスク軽減は、まず組織固有のリスクプロファイルを明確に把握することから始まります。現状を打破し大きな変化を起こすには、組織の従業員の状況が、同業種・同規模・同地域の他社と比べてどの程度の水準にあるのかを把握する必要があります。誰が最もリスクにさらされやすいのかを特定することで、行動変容に必要なタイムリーでパーソナライズされたセキュリティ対策(一人ひとりに合わせたトレーニングやリアルタイムのコーチングなど)を提供できるようになります。

KnowBe4の「業種別フィッシングベンチマーキングレポート」には、その第一歩を踏み出すために欠かせないデータがまとめられています。2026年度版を作成するにあたり、4,200万件のフィッシングシミュレーション、1,400万人のユニークユーザー、そして6万4,000の組織を対象とした網羅的な分析を行いました。また19の業種と7つの地域を対象に、Phish-prone™ Percentage (フィッシング詐欺ヒット率、PPP) を1年間にわたって調査・追跡しました。

その上で、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。

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

従業員がKnowBe4のセキュリティ意識向上トレーニングを開始します。その後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効果を測定します。

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。

2026年度 グローバルフィッシングベンチマーク

ベースラインテストでは、地域別のPPPが最も高いのはアフリカの35.9%で、次いで北米の34.5%、南米の31.5%と僅差で続きました。アジアは最も低い24.9%という結果となっています。これは、最初のテストを実施した時点ですでに意識向上トレーニングへの投資が他地域より進んでいたか、あるいは似たような性質の脅威が発生する環境であったことを示唆しています。

90日後のテストは地域によらず著しく均一な結果となり、16%から21.4%の範囲に収まっています。これは、開始時の状況に関わらず、初期トレーニングによって生じる短期的な行動変容が概ね同等であったことを示しています。

1年間にわたる継続的なトレーニングの結果、南米は地域別で最も低い3.3%というPPPを達成しました。これに北米の4%が続いています。アフリカは7.4%という、変わらず最も厳しい状況となっています。

	フェーズ1 ベースラインフィッシングセキュリティ テストの結果				フェーズ2 トレーニング開始後90日までの フィッシングセキュリティテスト結果				フェーズ3 トレーニング開始1年後から それ以降の フィッシングセキュリティテスト結果			
	1-249	250-999	1000-9,999	10,000+	1-249	250-999	1000-9,999	10,000+	1-249	250-999	1000-9,999	10,000+
組織の規模												
地域												
アフリカ	28.9%	30%	34.6%	39%	26.6%	28.1%	24.8%	14.7%	3.9%	15.1%	9.1%	3%
合計	35.9%				21.1%				7.4%			
アジア	23.1%	27.8%	28.4%	21.6%	18.6%	18.9%	19%	12.6%	6.6%	6.4%	5.8%	3.4%
合計	24.9%				16%				5.5%			
オーストラリア・ ニュージーランド	24.6%	28.5%	32.7%	54.5%	23.9%	24%	18.5%	16.7%	5.7%	5.5%	4.8%	4.3%
合計	33%				21%				5.3%			
ヨーロッパ	23.5%	26.1%	29.6%	38.1%	20.8%	22%	21%	21.6%	4.70%	4.5%	6.6%	4.7%
合計	31.1%				21.4%				5%			
北アメリカ	25%	29.5%	35.4%	44%	21.7%	21.9%	20.3%	16.6%	4.3%	3.9%	3.8%	4.2%
合計	34.5%				20.1%				4%			
南アメリカ	26.6%	25.4%	33.6%	32.9%	23.7%	21.5%	18.4%	12.8%	7.2%	3.6%	2.2%	2.8%
合計	31.5%				17.7%				3.3%			
英国・アイルランド	24.8%	26.8%	32.7%	33.1%	22.9%	23.1%	20%	14%	4.5%	5.5%	6.1%	5.8%
合計	30.3%				19.8%				5.5%			

アジア地域 2026年度版

著者: Dr. Kavin Boonyapredeedee, CISO アドバイザー

はじめに: アジアにおける脅威のランドスケープ

アジアのサイバーセキュリティ環境は、高まり続ける脅威にさらされています。アジアには世界でも有数の急成長を遂げるデジタル経済圏が存在しますが、その一方で、ますます巧妙化・執拗化するサイバー犯罪の拠点にもなりつつあります。急速なネットワーク化は計り知れない好機をもたらしましたが、地域内でのサイバーセキュリティ対策の成熟度にばらつきがあり、これが攻撃者に隙を与える要因となっています。そして急速なデジタルトランスフォーメーションと経済成長に伴い、この地域の企業は利益をもたらす格好の攻撃的となりました。たとえ技術的な防御策に多額の投資がなされていたとしても、組織のセキュリティの成否は、依然として「人」にあるからです。

生成AIを巧みに利用した攻撃は、自動化されたメールセキュリティゲートウェイをすり抜けるほど自然で、ターゲットの地域に最適化されたフィッシングメールを作成するようになっています。AIを駆使したディープフェイクや組織的な大規模詐欺、さらにはランサムウェアや情報窃取型マルウェアに至るまで、この地域が直面している課題は極めて深刻です。防御に対する責任は、これまで以上に従業員に重くのしかかっています。

組織と業界の概要

アジアのデータセットは、組織の規模を小規模（従業員数1～249名）、中規模（250～999名）、大規模（1,000～9,999名）、そしてエンタープライズ（10,000名以上）という4つの階層に分類されています。この地域には中小企業が多く、活気あるビジネス環境であることがわかります。その一方で、大企業の進出も着実に増えています。

2026年のベンチマークでは、アジア地域の平均基準PPPは24.9%と全地域の中で最も低い数値となりました。しかし、この全体的な数字だけでは、セクターレベルで生じている大きな差異はわかりません。ベースラインテストの結果、最も影響を受けやすいのは、法務（44.1%）、保険（41%）、教育（40.6%）の3業界でした。これらは、重要度の高い膨大なデータを扱う環境であり、機密性の高い顧客情報を保持しながらも、一方で正式な情報セキュリティ教育にあまり馴染みのない人々が多い業界でもあります。法律事務所においてベースラインが44.1%であるということは、トレーニングを導入する前の段階で、従業員の半数近くが模擬フィッシングメールを開いてしまっているということになります。

世界的に見ると、ストレス負荷が高く膨大なデータを扱う業界ほど、構造的に脆弱性が高い傾向にあります。特に大規模な医療現場では、脆弱性がベースラインで最大54%に達しています。アジアの法務、保険、および教育分野に属する組織は、自社の業務においても同様のリスクが当てはまると想定すべきでしょう。

ベンチマークデータの分析

アジアのすべての規模の組織を対象としたPPPのデータは、明確かつ希望の持てるものだといえます。継続的なトレーニングには効果があり、どのような組織規模においても一貫して成果を上げることが示されています。

ベースラインテストでは、この地域の平均PPPは24.9%でした。これは、トレーニングを実施する前段階では、従業員の約4人に1人が悪意のあるメールに反応してしまう可能性があることを意味しています。組織の規模が大きくなるほどリスクに晒される割合が上昇しており、小規模組織の23.1%から大規模組織では28.4%にまで達します。一方で、エンタープライズ組織では21.6%と、わずかに低下する傾向が見られます。大企業において基準値が高くなる傾向があるのは、おそらく組織が多くの部門や地域にまたがっているという複雑さが影響しています。こうした環境では、セキュリティに対する責任共有の意識が希薄になりやすいためです。

アジア

フェーズ1

ベースラインフィッシング
セキュリティテストの結果

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

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

1-249	23.1%	18.6%	6.6%
250-999	27.8%	18.9%	6.4%
1000-9,999	28.4%	19%	5.8%
10,000+	21.6%	12.6%	3.4%
全組織規模での平均PPP	24.9%	16%	5.5%

トレーニング開始から90日以内に、地域全体の平均値は16%まで低下します。特に改善が顕著なのはエンタープライズ企業で、21.6%から12.6%へと大幅に減少しています。この傾向は他の地域でも同様に見られるものです。体系化されたトレーニング体制を一元管理している規模の大きい組織は、一度プログラムを整えば一気に展開することができるからです。

1年以上にわたり継続的なトレーニングと模擬テストを実施した後では、地域全体の平均値は5.5%となりました。これはベースラインから相対的に78%減少したことを意味します。現時点では、組織の規模にかかわらずその結果は一貫しており、小規模組織が6.6%、中規模が6.4%、大規模が5.8%、そしてエンタープライズが3.4%となっています。継続的なトレーニングの結果、最終的に約5%という共通の数値に収束していく様子は、アジア圏のデータにおける最も顕著な傾向の一つです。これにより、本ベンチマークの全地域で確認された、「セキュリティ意識は、組織の規模を問わず、継続的な投資によって向上・測定が可能な能力である」という知見が裏付けられたことが分かります。

まとめ (確認ポイント)

→ ヒューマンリスクは共通して存在するが、業界ごとの偏りに注意

アジアの地域平均は24.9%と、全地域の中で最も低い水準にとどまっています。しかし、法務(44.1%)、保険(41%)、教育(40.6%)といった数値が示す通り、地域全体の数値が低く見えても、特定の業界では深刻な影響を受けている可能性があります。これらの業界に該当する組織は、自社の基準値を地域の標準よりもかなり高く設定する必要があるでしょう。

→ 組織規模によってリスクが変容

ベースラインのPPPは組織の規模が大きくなるにつれて上昇し、大規模組織では28.4%と最も高くなっています。コミュニケーションが複雑化し、使用ツールが増え、労働力も分散しているような大規模な環境では、その場しのぎの対応ではなく、体系化された継続的なトレーニングプログラムが不可欠です。

→ エンタープライズでは劇的に好転

エンタープライズ企業では、1年間のトレーニングの結果、ベースラインが21.6%から3.4%へと改善しました。これは、同地域の全組織規模の中で最も低く、長期的な数値です。一元管理されたトレーニングを大規模に計画的に実施することで、長期的かつ最も安定した成果を得られることが示されています。

→ 1年後の改善結果に期待

4つの組織規模のすべてにおいて、1年後のPPPの結果は3.4%から6.6%の範囲に集中しています。こうした一貫性は、技術的な防御策だけで実現できるものではありません。継続的なシミュレーション、迅速な改善、そしてセキュリティ意識が根付いた組織の文化の維持があってこそ、初めて達成されるものです。

→ 年に一度のコンプライアンストレーニングから、一歩先へ

フェーズ2(16%)とフェーズ3(5.5%)の結果にこれほどの開きがあることを見ると、トレーニングサイクルが1回だけでは不十分であることがわかります。セキュリティ責任者は、従来の、年に一度のコンプライアンス重視のプログラムから脱却し、各地域の状況に即した、継続的な攻撃シミュレーションとトレーニングに移行するべきでしょう。AIによって高度化し、特定の地域を標的にした脅威に対して、実効性のあるリスク低減を維持するためには、一歩踏み込むことが必要不可欠です。

KnowBe4について

KnowBe4は、現代の労働環境にあるお客様の企業の全従業員が、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。

セキュリティプロバイダーのパイオニアとして、デジタル化時代の人材である「AIエージェント」と「人」の両方を守る製品を提供し、世界の7万社を超える組織から支持を集めています。**KnowBe4プラットフォーム**は、攻撃シミュレーションとトレーニング、コラボレーションセキュリティ、そしてAIDA (Artificial Intelligence Defense Agents) と独自のリスクスコアを活用したエージェントセキュリティを提供しています。このプラットフォームは、15年間にわたる行動データを活用し、ソーシャルエンジニアリング、プロンプトインジェクション、シャドウAIなどの高度な脅威に対抗します。KnowBe4は、従業員とエージェント両方のセキュリティを確実に守ることで、信頼できる労働環境と進化する脅威に対する防御を実現し、セキュリティ分野を大きく牽引しています。

詳しくはwww.KnowBe4.jpをご覧ください。



KnowBe4 Japan合同会社 | 〒107-0052 東京都港区赤坂 9-7-1 ミッドタウン・タワー 18F
03-4586-4540 | www.knowbe4.com/ja | info@KnowBe4.jp

本書に記載されているその他の製品名および会社名は、各社の商標または登録商標です。