



Kaspersky
Security
Awareness

サイバーセキュリティの 文化を確立し、ビジネス の安全性を確保



セキュリティ意識が高い文化が重要である理由



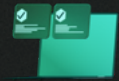
人為的なミス

侵害の62～80%は、人為的要因（ミス、権限の悪用、ソーシャルエンジニアリングなど）によって発生しています^{1,2}



499万ドル

データ侵害の発生時に、組織が負担するコストの平均額です³



コンプライアンスの観点から、セキュリティ意識の向上が、次のような基準や規則で義務付けられています：**PCI DSS、ISO/IEC 27001、GDPR、NIS 2**など。これらは、セキュリティ意識向上プログラムの実施による機密データの保護を要求、または強く推奨しています



85%以上

セキュリティ意識向上トレーニングの修了後に、警戒心や注意力が向上したと報告した従業員の割合。これは、インシデントの防止に役立つ行動変容の現れです⁴

90%

Kaspersky Security Awarenessの受講を他のユーザーにも推奨したいと考えるユーザーの割合⁴

300万

当社のトレーニングプログラムを正常に終了した従業員の数

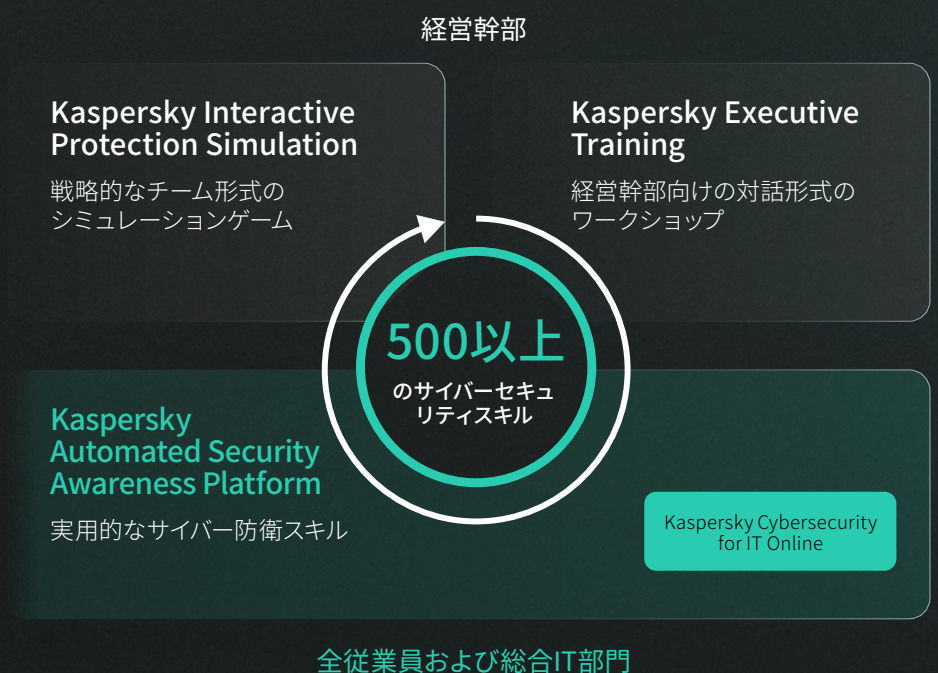
160以上

トレーニングソリューションで従業員を保護している組織が存在する国の数

Kaspersky Security Awarenessで、人為的なサイバーリスクを軽減

サイバー上の安全性を意識して行動する文化を、組織に浸透させましょう。強固なサイバーセキュリティ意識と実践的なスキルが、その基盤となります。これにより、人為的なミスによるインシデントの発生件数を減らすことができます。人的要因に対処する最善の方法は、適切かつ最新のコンテンツと、最新の学習方法と技術を組み合わせて構成されたトレーニングプログラムです。

Kaspersky Security Awarenessは、世界中のあらゆる規模の企業を対象としたソリューションです。従業員のサイバーリテラシーを向上させ、セキュリティに対する責任が全員にあるという文化の浸透を促進します。持続可能な行動変容には時間が必要です。そのため、当社では各種のツールや補強用の教材を使用して、継続的な学習サイクルを構築するアプローチを採用しています。例として、Kaspersky Interactive Protection Simulation、Executive Training、Automated Security Awareness Platform、Cybersecurity for IT Onlineなどがあります。



Kaspersky Security Awarenessを選ぶ理由

約30年間かけて培ったセキュリティの専門知識

Kasperskyのグローバルな専門知識を活用し、実用性が高いサイバーセキュリティトレーニングコンテンツを作成しています。新種の脅威の出現に応じて、当社のコンテンツも進化します。これにより、従業員が常に万全の態勢を維持できるようにサポートします。

行動変容の持続を支援

当社の方法論は、新しいスキルの強化、モチベーションの継続、学習成果が組織の定型業務に組み込まれることを支援します。

わかりやすい対話型の学習

当社のトレーニングでは対話型学習を採用しています。これにより、従業員は学習内容と日常業務を関連付けることができるようになり、知識の定着と実務への応用が促進されます。

組織全体にわたる高い関与性

経営幹部から現場スタッフに至るまで、あらゆる対象者に適した内容を、適切な形式で提供します。

1 2026 Data Breach Investigations Report, Verizon

2 2026 Cyber risk Survey (Kaspersky)

3 2026 Cost of a Data Breach Report (IBM)

4 2024 Security Awareness & Training Data Quadrant (Info-Tech Research Group)



Kaspersky Automated Security Awareness Platform

Kaspersky Automated Security Awareness Platform (ASAP) は、継続的なトレーニングが可能なオンラインツールです。従業員が実際の攻撃を認識し、阻止するためのスキルと知識を習得することができます。

Kaspersky ASAPは、世界トップクラスのエキスパートが開発するソリューションです。従業員のセキュリティ意識の向上と、ビジネスの強化を実現します：



人為的なインシデントの件数の削減

インシデントの結果生じる金銭的、評判上の損害も抑制します



コンプライアンス違反による罰金リスクの最小化

を、規制要件への準拠を通じて実現します



時間と労力の削減：

意識向上トレーニングの管理に必要な負荷を軽減し、ITチームの負担を緩和します

Kaspersky ASAPは、単なるフィッシング対策ツールではありません。MITRE ATT&CKテクニックに基づくトレーニングにより、従業員が防止可能な人間主導の攻撃ベクトルを示すことができます。例をご覧ください：

**MITRE
ATT&CK**

MITRE テクニック	脅威	スキルと行動面での成果
T1566：フィッシング	悪意のあるメール	フィッシング行為を認識し報告する
T1585：アカウントの設定	偽のアカウント / プロファイル	情報の共有前に信憑性を確認する
T1199：信頼関係	パートナーの信頼を悪用	不自然なリクエストに疑問を持つ
T1091：リムーバブルメディア経由の複製	リムーバブルメディア	USBメディアに存在し得るマルウェアの危険性を理解する
T1078：有効なアカウント	認証情報の盗難	ソーシャルエンジニアリングによるアクセス権限の付与を防止する

95%

トレーニング修了後、フィッシング攻撃を識別できるようになった従業員の割合

20倍

従業員が継続的にトレーニングを受講することで、抑制できるデータ流出の件数¹

ASAPで扱う主なトピック（これらに限定されません）：

Email

パスワードとアカウント

Webサイトとインターネット

PCセキュリティ

機密データ

個人情報

物理的なデータセキュリティ

GDPR

人工知能とニューラルネットワーク

経営トップへの攻撃

モバイルデバイス

ソーシャルメディアとメッセージ

サプライチェーン攻撃

産業用サイバーセキュリティ

銀行カードのセキュリティとPCI DSS

インシデントへの対応方法

フィッシング

グローバルな専門知識と柔軟性を活用し、従業員のセキュリティ意識向上を実現するトレーニング、評価、強化を実施

Kaspersky ASAPiには、あらゆる規模やセキュリティ意識のレベルの組織に適した3つのプランが用意されています。

		Essential 小規模なチームに最適 コンプライアンス対応のセキュリティ意識向上トレーニング	Proactive 成長中の企業に最適 予防的なセキュリティ意識向上トレーニングと効果測定	Advanced 特定の要件があり、セキュリティ文化が確立されている大規模企業に最適 カスタマイズ可能で実効性が高いセキュリティ意識向上トレーニング
フィッシング	カスタマイズ可能で現実に即したフィッシングシミュレーションにより、サイバー攻撃に対する従業員の対応力をテストします	●	●	●
エクспレスコース	対話形式のレッスンにより、人為的な脅威に対抗する実践的なスキルを育成し、組織がコンプライアンス要件を満たせる状態を維持します	●	●	●
メインコース	完全に自動化されたセキュリティ意識向上トレーニングは、リスクレベルに応じたカスタマイズが可能であり、マイクロラーニングやスキルの定着をサポートする要素も実装しています		●	●
コンテンツのカスタマイズ	カスタマイズ可能なモジュール、テスト、フィッシングページやドメインなど			●
オンプレミス導入	自社のインフラへの導入方法が選択可能です。これにより、機密データ、システム連携、企業コンプライアンスに関する完全な管理を確保できます			●

あらゆる規模の組織に対応した、効率的で管理しやすいトレーニング

- 

簡単なオンボーディング

簡単なオンライン登録で、最大5名のユーザーが2か月間デモ版を使用できます。利用開始ガイドとオンラインサポートも付属しています
- 

完全な自動化

トレーニングモジュール、テスト、フィッシングシミュレーションは、トレーニンググループの設定に応じて自動的に割り当てられます
- 

人的要因によるリスクを予防的に管理

Kaspersky SIEMやXDRとのシームレスな連携、サードパーティ製アプリケーションとの連携用APIにより、従業員の行動の全容を把握し、実際のセキュリティイベントに基づいたトレーニングをコンソールから直接割り当てることができます
- 

マルチテナントのサポートと管理者の役割の柔軟性

子会社や分散型チームを有する組織に最適です。一元的な監視が可能であると同時に、ローカルの管理者に管理を委任することができます
- 

事前定義されたカスタムルールに基づき、ユーザーを自動的にグループ化

役割別、部門別、リスクプロファイル別に体系化
- 

明確で、経営陣にも理解しやすいレポート

ダッシュボードには、各従業員の進捗、遅延、パフォーマンス低下などの基本的なデータをドリルダウン形式で表示し、ワンクリックで送信可能なPDFレポートを管理者に提供します
- 

柔軟な導入

SaaSプラットフォームとしての利用やオンプレミスインストールが可能
- 

シームレスな登録

Active DirectoryやOpenLDAPとの連携



Kaspersky Interactive Protection Simulation



相互理解の確立

意思決定者間の相互理解を促進します



可視化の支援

サイバーセキュリティのリスクを可視化し、売上や業務への影響を直接把握することができますようにします



チームの参加を促進

サイバーセキュリティの問題に対処し、セキュリティを最優先とする文化を醸成できるよう、チームの関与を促進します

KIPSは、あらゆる種類のITシステムや業務プロセスの使用に伴うリスクや課題に対する認識を向上させます。2時間の対話型のチームゲームで、上級管理職、業務システムエキスパート、およびIT担当者を対象としています。業界特有のシナリオを通じて、参加者は、Kasperskyのエキスパートが実際の攻撃キャンペーンで確認したサプライチェーン攻撃、サードパーティへのアクセスの悪用、ソーシャルエンジニアリング、マルウェアなど、最新の攻撃テクニックを体験することになります。時間と予算が制約される状況下で、各チームは戦略を立て、セキュリティインシデントの影響を予測し、効果的な対応を講じて、業績と収益を守る必要があります。

KIPS Live

娯楽性が高く、スタンドアロンイベントとして、または既存のカンファレンス、セミナー、企業イベントの一環として実施できる活動です。

- ・ 参加者は最大100名、各チーム4〜5名
- ・ 現場ファシリテーターおよびトレーニングアシスタント

KIPS Online

オンライン版は、グローバルな組織や公的な活動に最適です。KIPS Liveと組み合わせることで、遠隔地のチームを現地イベントに参加させることも可能です。

- ・ 最大300チーム（受講者は1000人まで）が、どこからでも参加可能

14種類の業界別シナリオ (今後も随時追加予定)

- IT
- 航空
- 企業
- 銀行
- 石油ガス
- 運輸業
- 発電所
- 浄水場
- 自治体
- 石油化学
- 石油販売
- 中小企業
- 電気通信業
- 技術的帰属



KIPSでカスタマイズ可能な要素

- ・ 共同ブランドまたは顧客ブランドのボード、カード、テーブル番号
- ・ Kasperskyと提携して構築された独自のシナリオで、お客様のネットワークや過去のインシデント、特定の業界固有の脅威を再現することができます



Kaspersky Cybersecurity for IT Online

Cybersecurity for IT Online (CITO) は、サービスデスク担当者、システム管理者、ITセキュリティチームで専任ではないメンバーを対象とした、対話型トレーニングプログラムです。本コースでは、実践的なスキルを習得することができます。具体的には、日常的なPCのインシデントの中に潜むサイバー攻撃の検知、関連データの収集、およびサイバー防衛の第一線としての行動が挙げられます。

受講者は、簡潔な理論と実践的なヒントを組み合わせた6つのモジュールを進めていきます。各モジュールには4〜13種類の演習が用意されており、実際のITセキュリティツールや日常的な業務に焦点を当てる内容となっています。

悪意のあるソフトウェア

望ましくないプログラムとエクスプロイト

サーバーのセキュリティ

調査の基礎

フィッシングとオープンソースインテリジェンス

Active Directoryのセキュリティ

インシデントレスポンスとセキュリティ強化の実践的なスキル：



マルウェア、望ましくない可能性のあるプログラム、脆弱性攻撃、およびフィッシング攻撃を検知し、分析し、対処する方法を学習します



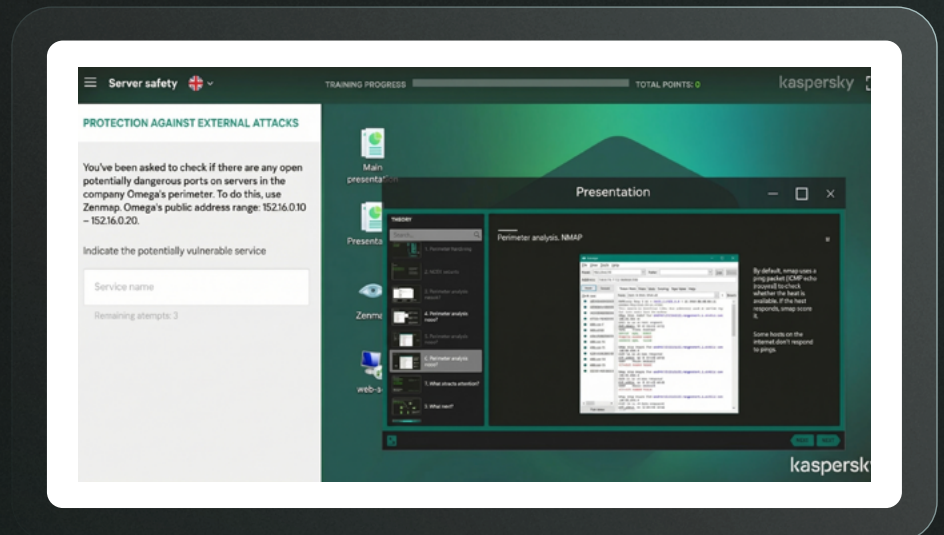
実務で活用できるツールやテクニックを応用し、ITインフラのセキュリティを強化するとともに、インシデントを効果的に調査します



ログ分析、デジタルエビデンスの収集、脅威の調査に関するスキルを養成します



ハードニング、ポリシー設定、運用監視を駆使してサーバーとActive Directoryのセキュリティを確保する方法を習得します



Kaspersky Executive Training

経営陣の意思決定が、リスク管理態勢、企業コンプライアンス、組織の長期的なレジリエンスに直接与える影響を示すことで、トップダウン型のセキュリティ文化の浸透を推進します。Kaspersky Executive Trainingは、事業責任者や経営幹部を対象としたライブワークショップです。

現在の脅威の状況が事業にどのような影響を与えるか、サイバー攻撃が発生した場合にどのような対応が必要かなど、多岐にわたる内容について解説します。このトレーニングは、KIPSとの併用によって理想的な効果を発揮します。

業務に不可欠なサイバーセキュリティの要素について、技術用語を使用せず、明確で理解しやすい言葉で解説します：



サイバーセキュリティがシステム全体の一部であることの理解



サイバーリスクが事業運営に与える影響と、その管理方法の学習



サイバーセキュリティガバナンスにおける経営幹部の役割の理解

サイバーセキュリティの文化の醸成

真のサイバーレジリエンスには、ポリシーや技術だけでなく、文化が不可欠です。その文化は、人々の行動、リーダーの指導方法、プロセスの設計、技術がそれらすべてを支える仕組みによって形成されます。



人々と行動



リーダーシップ
と協力

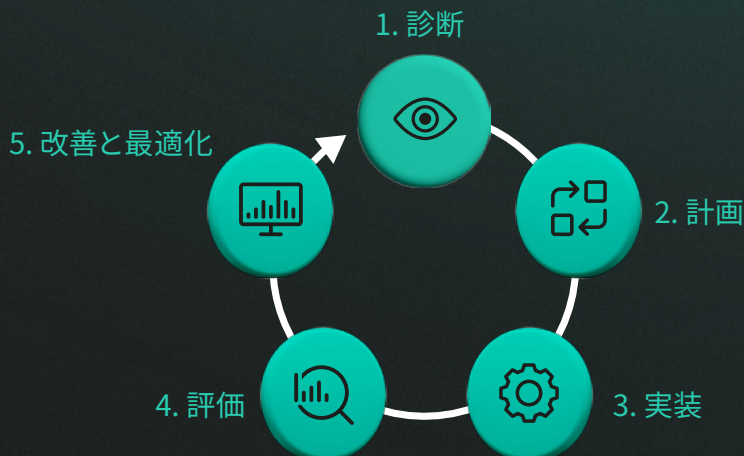


運用の統合



セキュリティの整備と
準備態勢

持続的なサイバーセキュリティの文化は、継続的な取り組みを通して実現されます。そこで当社は、Kaspersky Security Awarenessソリューションを使用可能とする、5つの重要なステップに基づいた体系的なアプローチを開発しました。



組織におけるサイバーセキュリティ文化は、現在どの程度成熟していますか？

0

断片化

リスク：基本的な慣行や体制が欠如していることで、脆弱性が極めて高くなります。軽微なインシデントであっても、深刻な結果に発展する可能性があります。

1

アドホックな態勢

リスク：明示的なルールのみが遵守されます。想定外の状況では、従業員は自身の判断に基づいて行動します。

2

管理者による管理

リスク：インシデントの件数は減少傾向にありますが、複雑なシナリオに対しては依然として脆弱な状態が続いています。

3

統合的な運用

リスク：プロセスは問題ないように見えますが、サイバー文化が自己調整システムとして機能しない場合、「遅延リスク」が解消されません。

4

高いレジリエンス

結果：インシデントの件数と深刻度が、継続的に減少します。組織は、刻々と変化する脅威の状況にすぐに対応することができます。

”

セキュリティが一時的な取り組みではなく、組織の文化として定着すると、リスクは低減し、それに伴う成果も現れます。

CISO

顧客エンゲージメントサービス

無料での試用を開始して、自社のセキュリティ文化のレベルを評価してみましょう



Kaspersky Security Awareness

危機意識と組織の
安全性を向上

www.kaspersky.co.jp

© 2026 AO Kaspersky Lab.
登録商標およびサービスマークは、各所有者の財産です。

#kaspersky
#truetobusiness