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

kaspersky cybersecurity
true to business

人為的なミス

最大の脅威：平均して、侵害の64～86%は悪意のない人的要因によるものです[1]

440万ドル

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[2]

セキュリティ意識向上を要求する規則

コンプライアンスの一環として、機密データの保護を目的としたセキュリティ意識向上プログラムの実施を強く推奨している法律、指令など： PCI DSS、ISO /IEC 27001、GDPR、NIS 2

セキュリティを意識した企業文化の醸成がもたらす成果

Kasperskyの調査によると、セキュリティ意識向上トレーニングを受講した従業員の85%以上が、警戒心や注意力が向上したと報告しています。これらは、インシデントの防止に役立つ行動変容が成果として表れている証拠と言ってよいでしょう。

92%

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

300万

当社のトレーニングプログラムを正常に修了した従業員の数

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

人為的なサイバーリスクを軽減する効果的なアプローチ

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 ソリューション

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がお客様に選ばれる理由

現実の脅威を発見し、対応するスキルと自信の定着を支援

Kasperskyが30年近く蓄積してきた専門知識とリアルタイムの脅威インテリジェンスを駆使し、実践的なサイバーセキュリティトレーニングの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。

わかりやすい対話型の学習

当社のトレーニングは、明確で論理的な構造を持つ対話型学習を導入しています。これにより、従業員はレッスンと日常業務を関連付けることができるようになり、理解度や定着性、実際の業務への応用力が向上します。

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、組織の定型業務への学習成果の組み込みを支援します。その結果、行動が持続的に変化し、セキュリティを意識した行動が自然にできるようになります。

組織全体にわたる高い関与性

ハイレベルで実用的な洞察を必要とする経営幹部から、実践的な指導を必要とする現場スタッフまで、あらゆる対象者に適切なコンテンツを適切な形式で提供します。

1 Kaspersky Human Factor 360 Report, Cybersecurity Ventures, Verizon Data Breach Reports
2 Cost of a Data Breach Report 2025（IBM）

Kaspersky Automated Security Awareness Platform：人為的ミスを防止するファイアウォール

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。このツールにより、従業員が実際の攻撃経路を認識し、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：

人為的な要因によるインシデントの発生件数を抑制し、結果的に発生する経済的・風評的損害を軽減

企業コンプライアンス要件のサポートにより、コンプライアンス違反による罰金の発生リスクを最小限に抑えます。

意識向上トレーニングの管理に必要な時間と労力を軽減し、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テクニックに対応したトレーニングにより、従業員がどのような人間主導の攻撃ベクトルを防ぐことができるかを把握することができます。以下に例を示します：

MITREテクニック	脅威	習得するスキルと行動の変化
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、抑制が可能なデータ流出の件数[1]

ASAPで扱う主なトピック（これらに限定されません）：

- メール
- 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ンジャー
- サプライチェーン攻撃
- 産業用サイバーセキュリティ
- バンク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
- ヴィッシング

技術的なツールに加えて、従業員が多層的な保護の新たな一部としての役割を果たす環境を実現します。

試用を開始

1 Kaspersky Automated Security Awareness Platform Research（2025年）

知識の定着とスキルの応用を促進するコンテンツと方法論

エキスパートの専門知識を活用

コンテンツは、約30年にわたるサイバーセキュリティの専門知識と、実践的で不可欠なサイバーセキュリティスキルを複数のテーマにわたって網羅するコンピテンシーモデルに基づいて構築されています。

多彩なコンテンツ

対話型モジュールや演習、実際のケース、テスト、動画、マルチシナリオのフィッシングシミュレーションを通じて、知識の定着をサポートします。

カスタマイズ可能な幅広いオプション

ロゴやブランド認定証の追加、社内用スライド、文書、ポリシーによるレッスンの拡充、カスタムSCORM/PDFモジュールの追加、テスト構成の調整。

ヒューマンセントリックな設計

人間がどのように情報を吸収、保持、適用するかという観点を中心に設計されています。

仕組み

組織の全員がサイバーセキュリティのリスクを認識する必要がありますが、その知識の深度は役割やリスクプロファイルによって異なります。これが、画一的なトレーニングが失敗する原因です。当社のプラットフォームは、500種類を超える実践的なスキルの習得、スタッフのグループ化、各受講者への適切なトレーニングの割り当てを、わずか数クリックで行うことができるよう、下記のコンポーネントを使用してチームを支援します。

メインコース

難易度別に分類されたマイクロレッスンを通じて、詳細な知識を習得します。

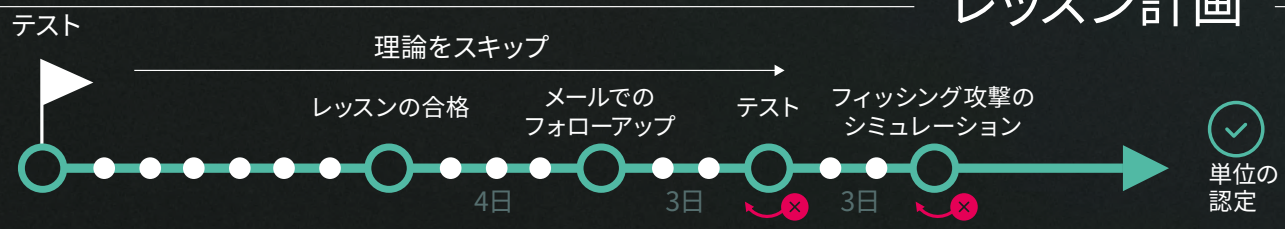
エクスプレスコース

サイバーセキュリティトレーニングのコンプライアンス要件を迅速に満たします。また、没入感が非常に高く、短い音声や動画によるトレーニングを活用して、最新の知識を習得することもできます。

フィッシングシミュレーター

トレーニング前、トレーニング中、トレーニング後にフィッシング攻撃のシミュレーションを実施し、サイバー攻撃に対する従業員の抵抗力をテストします。

レッスン計画



各種の活動を組み合わせたブロックにより、**記憶効果を最大化**

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

オンラインで登録すると、2か月間、最大5ユーザーまでのデモ機能を使用することができます。 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一方、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

明快なレポート

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。

柔軟性が高い導入が可能

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

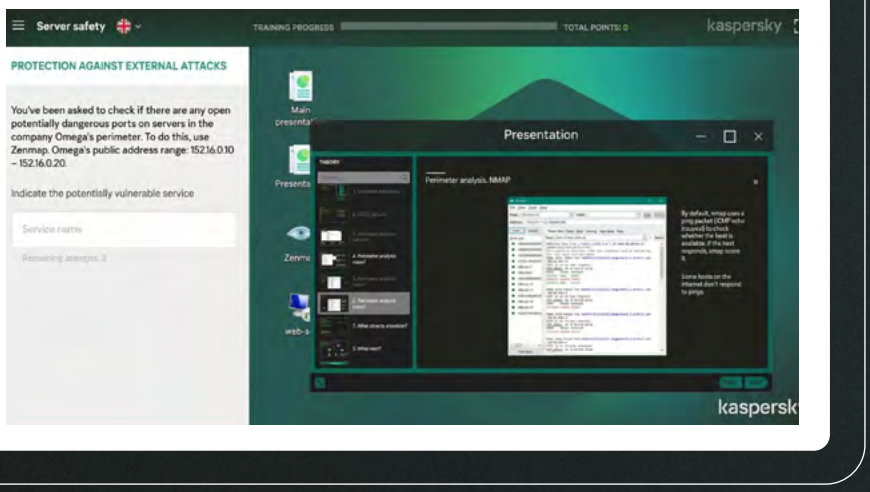
Active DirectoryやOpenLDAPとの連携

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、および専任ではないITセキュリティチームの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。日常的なPCインシデントにおける隠れたサイバー攻撃の検知、関連データの収集、サイバーセキュリティ防衛の最前線としての役割を果たすための実践的なスキルを身につけることができます。

基本レベルのインシデントレスポンスのための実践的なスキル：

- 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、フィッシング攻撃の検知、分析、および対処の方法を習得します
- 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



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脆弱性攻撃	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

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。サイバーセキュリティの中核的な原則に加えて、参加者はセキュリティ投資の経済的妥当性について重要な洞察を習得することが可能です。これにより、経営幹部はセキュリティ対策と業績の向上を関連付ける視点を養うことができます。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

Kaspersky Interactive Protection Simulation（KIPS）：ビジネス視点からアプローチするサイバーセキュリティ

KIPSは、あらゆる種類のITシステムや業務プロセスを使用すること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、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、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最新の攻撃テクニックを体験します。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。

- 意思決定者の間で合意を形成します
- サイバーセキュリティのリスクを可視化し、売上や業務に直接関連付けて把握することを支援します
- 各チームにサイバーセキュリティの問題への関与を促し、セキュリティ重視の文化を醸成します

KIPS Live

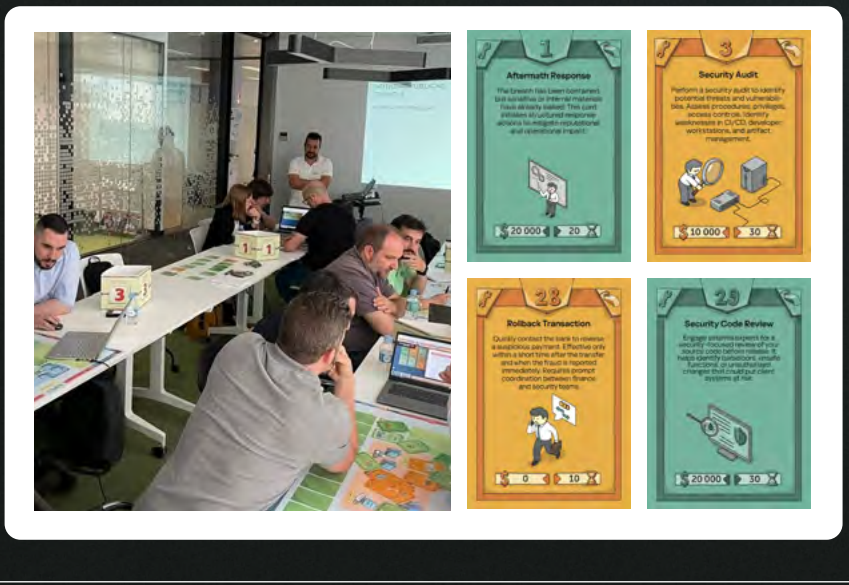
娯楽性が高く、スタンドアロンイベントとして、または既存のカンファレンス、セミナー、企業イベントの一環として実施できる活動です。

- 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



業界固有の14件のシナリオ（随時追加予定）

- 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
- 技術的なアトリビューション
- IT

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

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

持続可能なサイバーセキュリティ文化は、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：明示的に定められた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。

“

セキュリティが単なる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

Kaspersky ASAPを導入し、従業員、プロセス、技術の連携を強化することで、強靭なサイバーレジリエンスを実現する文化の形成に、今すぐ取り組みましょう。

今すぐ試す

Kaspersky Security Awareness

危機意識と組織の安全性を向上

www.kaspersky.co.jp

#kaspersky
#cybersecuritytruetobusiness