従業員にとって楽しく、マネージャーにとっては効率的

Kaspersky ASAP: Automated Security Awareness Platform

評価版
k-asap.com/ja

kaspersky bring on the future

Kaspersky Automated Security Awareness Platform

Kaspersky ASAP: Automated Security Awareness Platform

サイバーインシデントの82%がヒューマンエラーによるもので、結果として企業に莫大な損害を与えています。従来のトレーニングプログラムはこの問題に対処するように作られていないため、新しいアプローチが必要になります。それが、Kaspersky ASAPです。

ヒューマンエラーは最大のサイバーリスク

79%
の従業員
が、過去1年間に、リスクを認識しているにもかかわらず、リスクのある行動を少なくとも1回したと回答*

51%
の従業員
が、サイバー攻撃の被害から企業を守る責任はIT部門がすべて負うべきだと回答*

55%
の大企業
が、従業員による不適切なIT利用に起因する脅威を報告**

51%
の中小企業
が、従業員によるITセキュリティポリシー違反に起因するセキュリティインシデントを体験**

26%
の従業員
が、個人のメールアドレスと仕事で使うアカウントで同じパスワードを使用していると回答***

効果的なセキュリティ啓発プログラムの立ち上げを阻む要因

企業はセキュリティ啓発プログラムの導入に前向きですが、その多くが、プロセスにも結果にも不満を抱えています。とりわけ、必要な経験や資源が乏しい中小企業にとっては難しい課題となっています。

受講者にとって非効率的

難しくてつまらない、無意味な手間である

方法ではなく禁止事項ばかり学ぶ

知識が身につかない

読んだり聞いたりするのは実践より効果が薄い

管理者にとっての負担

プログラムを作り、目標を設定する方法は？

トレーニングの割当を管理する方法は？

プログラムを管理する方法は？

スタッフが積極的に学んでいることを確認するには？

* 「Balancing Risk, Productivity, and Security」、Delinea（2021）

** 「ITSecurity Economics 2022」、カスペルスキー

*** https://www.beyondidentity.com/blog/password-sharing-work

あらゆる規模の組織のための効率的で管理しやすいトレーニング

Kaspersky ASAP（Automated Security Awareness Platform）は、Kaspersky Security Awarenessトレーニングポートフォリオの中核となるプラットフォームです。このプラットフォームは、年間を通じて従業員に強力で実践的なサイバー防衛スキルを身に付けてもらうためのオンラインツールであり、**組織における人為的なサイバーインシデントを減らすのに役立ちます。**

プラットフォームの起動や管理のために特別なリソースや環境は必要なく、会社の安全なサイバー環境の構築に向けて学習を進める工程ですべての段階にヘルプが用意されています。

見逃せない有意義なコンテンツ

啓蒙プログラムを選ぶうえで最も重要な基準の1つが効率性です。ASAPなら、効率性を考えたトレーニングコンテンツで、効率的に管理できるようになっています。コンテンツは**25年以上にわたって蓄積されたサイバーセキュリティ**の経験に基づいており、すべての従業員が備えているべき**実践的かつ基本的な350以上のサイバーセキュリティスキル**から構成されたコンピテンシーモデルとしてまとめられています。

サイバーセキュリティについて学ぶ機会を従業員に提供しましょう。
従業員の態度や行動の変容が、貴社のビジネスとITシステムを守ります。

効率的なトレーニング

一貫性	– よく考えて構成されたコンテンツ – スキルが確実に身につく、対話型のレッスン、継続的な強化、テスト、フィッシング攻撃のシミュレーション トレーニング教材のコンテンツと構成には、人間の記憶力の特徴や、情報を吸収・維持する能力が考慮されています。
実践的で楽しい	– 従業員の毎日の業務に関係する内容 – すぐに使えるスキル 従業員が個人的に関心を持てる実際的な状況を例にしているので、学習への関心が高まり、情報を記憶に残すことができます。
前向き	– 安全のための行動を事前に実行 – やってはいけないことだけではなく、「理由」と「方法」を説明 ルールや制限が多すぎると不満が生まれて消極的になりますが、説明し、納得させると、人々は対応および行動の変容につながる方法を自然に考えるようになります。

管理が簡単

管理が簡単	– 学習管理が完全に自動化されているため、プラットフォーム管理者が介入しなくても、それぞれの従業員が自分のリスクプロファイルに応じてスキルをレベルアップ できます。 – AD（Active Directory）との同期、SSO（シングルサインオン）、オープンAPI（サードパーティソリューションとの連携を実現）、初回アクセス時のオンラインオンボーディング、FAQセクション、ヒントなどにより、プラットフォーム管理の利便性と効率が向上します。
コントロールが簡単	「オールインワン」のダッシュボードと実践的なレポート： – レッスンの進捗に関するレポート – テストとフィッシング攻撃のシミュレーションに関するレポート
楽しみながら学べる	招待状やリマインダー、レポートが受講者と管理者に自動で送信されます。

提供オプション

Kaspersky ASAPには、お好みに応じて次の3つの提供オプションがあります。

- **完全オンラインのクラウドベースソリューション。**この場合、ユーザーのデータは選択されたサーバー所在地に応じて適用される法規制を完全に遵守して処理されます。例えばヨーロッパを選択した場合、データはEU（ドイツ、フランクフルト）で保存され、法的に保護されるすべてのデータはEU一般データ保護規則（GDPR）に従って処理されます。
- **SCORMパッケージのコンテンツ。**このオプションでは、トレーニングモジュールを社内のLMS（学習管理システム）と統合できます。ただし、このオプションにはテストとフィッシング攻撃のシミュレーションが含まれない点に注意してください。
- **オンプレミス。**このオプションは、機密性を最大限に確保したいお客様向けです。何らかの法規制を遵守する必要がある企業にとって、オンプレミスへの導入はコンプライアンスをサポートするため、多額の罰金や罰則を回避することができます。顧客の社内ネットワークにコースウェアが導入され、サーバーのハードウェア、データセキュリティ、設定を完全に管理できます。インターネットに接続していないユーザーもトレーニング資料にアクセスできます。

ASAPの管理：完全自動化により操作が簡単

4ステップでプログラムをスタート

1

ユーザーの追加

AD同期を使用するか、.xlsxファイルをアップロードまたは手動で追加

2

ユーザーのグループ分け

ユーザーを手動で分類するか、必要なターゲットレベルに基づくルールで分類

3

トレーニングの開始

ユーザーを手動で分類するか、必要なターゲットレベルに基づくルールで分類して、各グループに開始日を設定

4

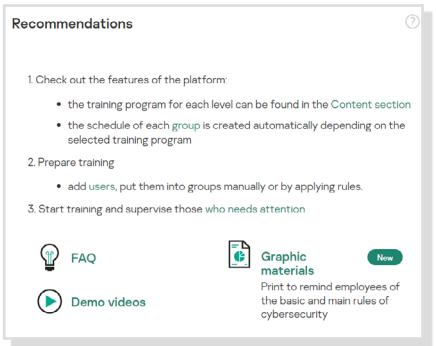
ASAPによる自動トレーニング管理

ASAPが各グループのスケジュールや招待状、リマインダー、その他のコミュニケーションのスケジュールを設定し、すべて自動で実行

トレーニングへのアプローチを刷新

Kaspersky ASAPは、サイバーセキュリティ学習コンテンツの提供方法を刷新します。従業員に基本的な**エクスプレスコース**を割り当てて、サイバーセキュリティトレーニングの規制要件に迅速に対応したり、従業員の知識をリフレッシュしたりすることも、複雑な内容を詳細に学べる**メインコース**を割り当てることもできます。

初回ログイン中のオンボーディング、推奨事項、FAQ、さらにはプラットフォームの仕組みを管理者とユーザーの視点から説明するデモ動画など、学習プロセスを開始するのに必要なすべてが管理用のメインページに用意されています。



対応トピック

対応トピック

メインコース	エクスプレスコース
メール	メール
パスワードとアカウント	パスワードとアカウント
ウェブサイトとインターネット	ウェブサイトとインターネット
ソーシャルメディアとメッセンジャー	モバイルデバイスセキュリティ
PCセキュリティ	ソーシャルメディア
モバイルデバイス	自分のコンピューター
機密データの保護	機密データの保護
個人情報	ドクシング
GDPR	暗号通貨のセキュリティ
産業向けサイバーセキュリティ	リモートワーク時の情報セキュリティ
銀行キャッシュカードのセキュリティとPCI DSS	連邦法152-FZ（ロシア）
物理的なデータセキュリティ	連邦法FZ-187（ロシア、重要な情報インフラのセキュリティ）

トピックは大型のブロックに分類され、ITセキュリティに関連するさまざまなトピックを網羅しています*。

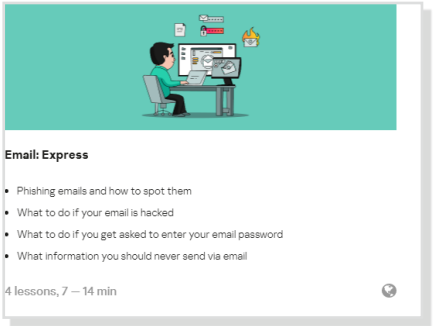
#パスワード #フィッシング #会社アカウント #危険なメッセージ #キャッシュカード #ランサムウェア #ソーシャルエンジニアリング #危険なファイル #ブラウザーを使う #企業倫理 #アンチウイルス #悪意のあるソフトウェア #アプリケーション #ブラウザー #機密情報 #情報の保存 #情報の送信 #個人情報 #インターネットと法律 #欧州の法律 #ビジネス #危険なリンク #偽のウェブサイト #ランサムウェアサイト #バックアップ #モバイルデータ #暗号化 #クラウドサービス #産業スパイ #PCI DSS #二要素認証 #デジタルフットプリント #Torrent #キャットフィッシング #標的型攻撃 #ハッシュ #トークン #パターンロック #マイニング #ペアレンタルコントロール

* トピックやコンセプトの最新のリストはこちら：k-asap.com/ja

それぞれのトピックは複数のレベルで構成されており、セキュリティスキルが具体的かつ詳細に説明されています。レベルは、排除したいと望むリスクの程度に応じて決まります。たとえば、単純な攻撃や一点集中型の攻撃から保護する必要がある場合、通常はレベル1で十分です。より高度な標的型攻撃から保護する方法を学びたい場合には、それより上のレベルが必要になります。

例：「ウェブサイトとインターネット」トピックで学ぶスキル

初心者 （費用のかからない、簡単な）一点集中型の攻撃を回避する	初級 具体的なリスクプロファイルに基づいて 一点集中型の攻撃を回避する	中級 よく準備された、狙いを絞った攻撃を回避する	上級* 標的型 攻撃を回避する
以下を含む、23のスキル： – 偽のポップアップを識別する – リダイレクションに注意する – 本物のダウンロードリンクと偽のリンクを見分ける – ウェブ上の実行可能ファイルを識別する – ブラウザ拡張機能の信頼性を判断できるようになる	**以下を含む、34のスキル：** – 有効なSSL認証のあるサイトでのみデータを入力する – 登録するたびに異なったパスワードを使う – いくつかの特徴から、偽サイトを識別する – 数字を使ったリンクを避ける – 偽のサブドメインによる、無効なネットワークリンクアドレスを識別する	**以下を含む、12のスキル：** – 送信前に共有するリンクをチェックする – Torrentには、信用できるメーカーのソフトウェアだけを使う – Torrentからは、正当なコンテンツのみをダウンロードする – ブラウザーのCookieを定期的に消去する	**以下を含む、13のスキル：** – 巧妙な偽リンク（会社のウェブサイトのように見えるリンク、リダイレクトするリンクなど）を識別する – 特殊なユーティリティを使ってサイトをチェックする – ブラウザーがマイニングしているかどうかを識別する – ブラックSEOサイトを避ける
	+ 初級スキルの強化	+ 過去のスキルの強化	+ 過去のスキルの強化

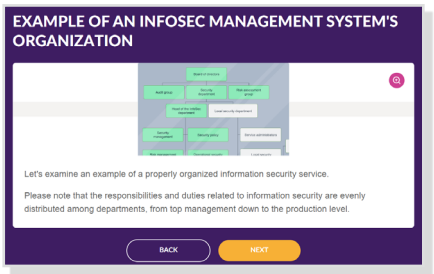


ASAPエクスプレスコース

音声動画形式の短期トレーニングコースです。サイバーセキュリティの各トピックに複数の短いレッスンが含まれており、ユーザーはサイバーセキュリティの基本スキルを理解できます。

- インタラクティブな理論
- 動画
- テスト

フィッシング攻撃のシミュレーションは学習パスに含まれていませんが、管理者が個別に割り当てることは可能です。



ASAPメインコース

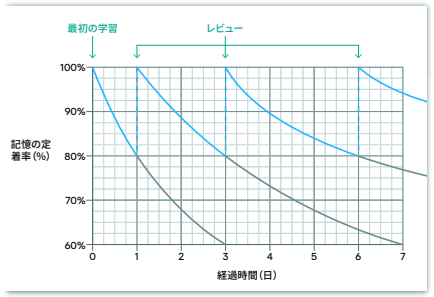
人間の記憶力の特徴を踏まえたトレーニング：

- マルチモーダルなコンテンツ：
  - 各ユニットに含まれているもの：インタラクティブなレッスン、強化、評価（テストと、場合によってはフィッシング攻撃のシミュレーション）
  - すべてのトレーニング要素が各ユニットで学ぶ特定のスキルに対応しているため、スキルを真の意味で理解でき、新しい求められる行動の一部になる

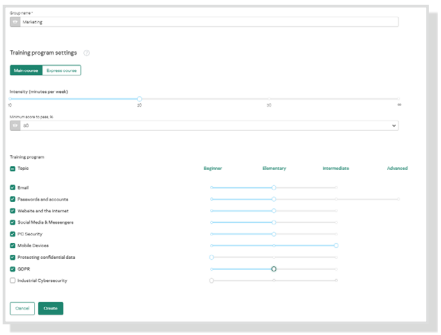
- インターバル学習：
  - 特定のインターバルでトレーニング要素間の振り返りを行うため、ただクリックするだけのレッスンが排除され、記憶が定着しやすい。インターバルはエビングハウスの「忘却曲線」の研究に基づく
  - 繰り返しが、安全な習慣を身につけさせ、忘れるのを防ぐ

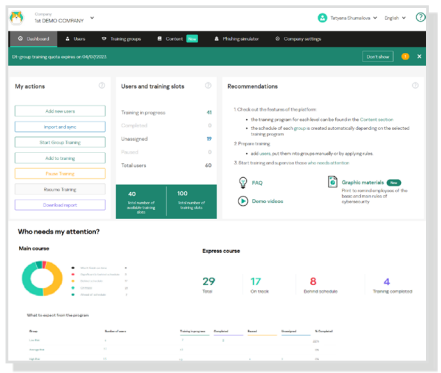
- 実際の状況とマッチするバランスのとれた構造のコンテンツで、効率的な学習を実現：
  - 従業員にとってのサイバーセキュリティの個人的な重要性を強調する、実際の状況に即した例を豊富に利用
  - 知識を与えることだけではなく、スキルを教えることに主眼を置いているため、実践的な演習や従業員関連のタスクが各モジュールの核となっている

エビングハウス「忘却曲線」



フレキシブルなラーニングパス





フレキシブルな学習

トレーニングの範囲は完全にフレキシブルでありながら自動化されており、一連の学習管理の効果を維持することが可能です。それぞれのトレーニンググループに対して、次の内容を選択できます。

- メインコースまたはエクスプレスコース、あるいは両方の組み合わせ
- 当該グループのメンバーがメインコースやエクスプレスコースで学ぶべきトピック
- メインコースに選択した各トピックで受講者に求める目標達成レベル

これらの設定に基づいて、各受講者グループの学習パスが自動的に構築されます。

ダッシュボードですべて管理

- トレーニングを管理するために必要なこと（統計、ユーザーのアクティビティと進捗の概要、トレーニングスロット、グループトレーニング、結果を改善するための提案）をダッシュボードですべて実行できます。ワンクリックでレポートをダウンロードでき、レポートの頻度もそこで設定できます。

自由に学習

- 従業員はいつでも都合のよい時間に好きなデバイスを使って学ぶことができます。ASAPはモバイルフレンドリーなデザインなので、楽しく快適に学習できます。
- ユーザーはトレーニングの招待状に記載された個人用のリンクからトレーニングポータルにアクセスすることも、管理者が設定していればSSO（シングルサインオン）技術を使ってすべてのユーザー用の単一のリンクからアクセスすることもできます。

カスタマイズ

管理者は次のような方法でプログラムの外観を簡単に変更できます。

- 管理パネル、トレーニングポータル、プラットフォームメールのカスペルスキーロゴを自社のロゴに置き換える
- 認定証をカスタマイズする
- レッスンに個人的なコンテンツを追加する

統合

オープンAPIを使用してサードパーティのソリューションとやりとりできます。オープンAPIはHTTP経由で機能し、複数の要求/応答メソッドを提供します。

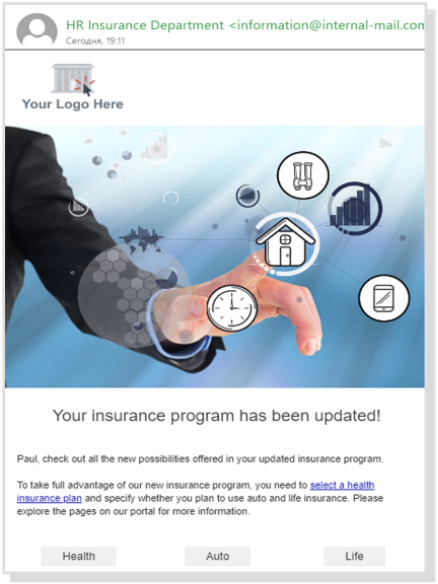
ASAPはKaspersky KUMAおよびXDRプラットフォームと連携します：
– 管理者はXDRのイベントを確認して、ASAPでのトレーニングの割り当てを含む適切な対応をとれます
– インシデントカードに、攻撃されたユーザーの意識レベルに関する情報が補足として提供されます

ローカライズ

ASAP は 25 の言語で使用できます*。ASAPのローカライズは単なる翻訳の域を越えており、テキストやビジュアルをさまざまな言語に翻訳したうえで、さまざまな文化や現地の考え方と照らし合わせて調整しています。

* 現在利用可能な言語のリストはこちら：
k-asap.com/ja

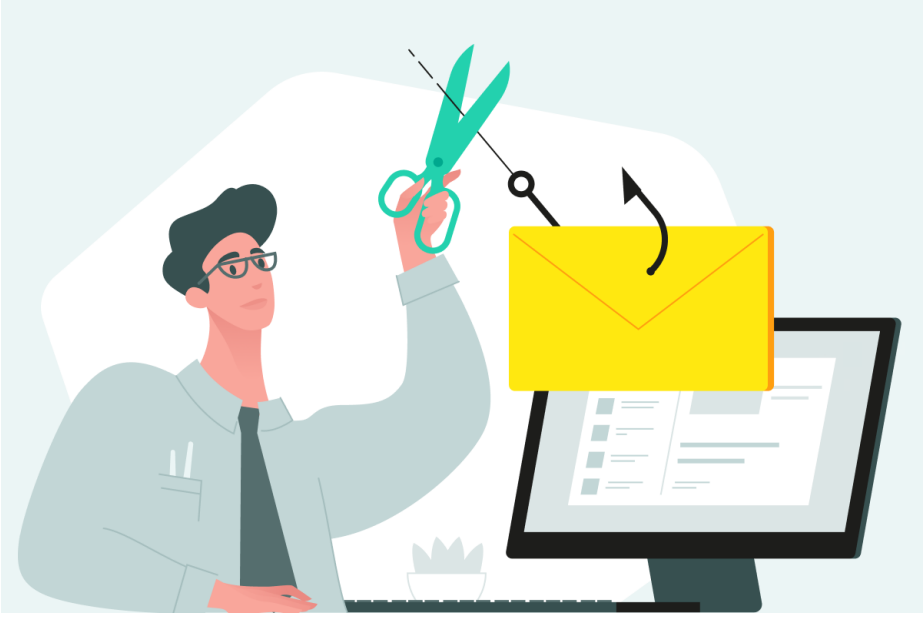
編集可能なフィッシングシミュレーションのテンプレートとフィードバックの例



フィッシング攻撃シミュレーション

メイントレーニングに加えてフィッシング攻撃シミュレーションも提供されています。このシミュレーションでは、従業員がフィッシング攻撃を回避する実践的なスキルをテストすることで、トレーニングマネージャーがユーザーの知識のギャップを速やかに認識し、問題のあるトピックについてさらなる学習を促せるように支援します。また、潜在的に危険な兆候を認識する方法を従業員に教え、従業員の知識を実践に移すための優れたツールにもなります。

プラットフォームには、フィッシングの例が含まれる既製のメールテンプレートも用意されており、利用可能なすべての言語でユーザーに送信できます。テンプレートは定期的に更新され、新しいテンプレートが追加されます。さらに、事前定義されたテンプレートをベースに、カスタムのメールを作成することも可能です。



フィッシング攻撃のシミュレーションをトレーニング開始前に行ってみて、従業員の対応能力をチェックしましょう。そうすることで、従業員と経営陣がトレーニングのメリットを把握できるようになります。

従業員は、フィッシング攻撃のシミュレーションに騙されることなく、**「フィッシング報告」ツール**を使ってフィッシングメールを報告することで、トピックの理解度を実証できます。

「フィッシング報告」ツールは、従業員の意識レベルを示し、受信ボックスからメールを削除し、プラットフォーム管理者だけでなくIT部門やITセキュリティ部門にもメッセージを送信することで、フィッシングに対する組織の検知・応答のレベルの改善に役立ちます。

MSP/MSSPパートナーや地理的に分散した体系をとる企業向けのKaspersky ASAP

このプラットフォームでは、マルチテナンシーに対応した単一のコンソールから複数の会社を対象に意識啓発トレーニングを展開、管理することができ、追加のソフトウェアを使用する必要はありません。

幸い、Kaspersky ASAPにはライセンスクォータ管理機能があり、これを使用すると会社ごとに特定の有効期間でライセンスクォータを割り当てることができます。

また、会社ごとに管理者を追加し、異なるロールを割り当てることも可能です。

Kaspersky Security Awareness – ITセキュリティスキルを身につけるための 新しいアプローチ

プログラムの主な特長

サイバーセキュリティに関する豊富な知識
25年以上におよぶサイバーセキュリティの経験が、製品の中核となるサイバーセーフティースキルセットとなっています。

組織のあらゆるレベルで従業員の行動を変えるトレーニング
ゲーム形式のトレーニングは、エデュテイメントを活用した学習意欲のわく内容です。サイバーセキュリティスキルを定着させる学習プラットフォームにより、学んだスキルを確実に習得できます。

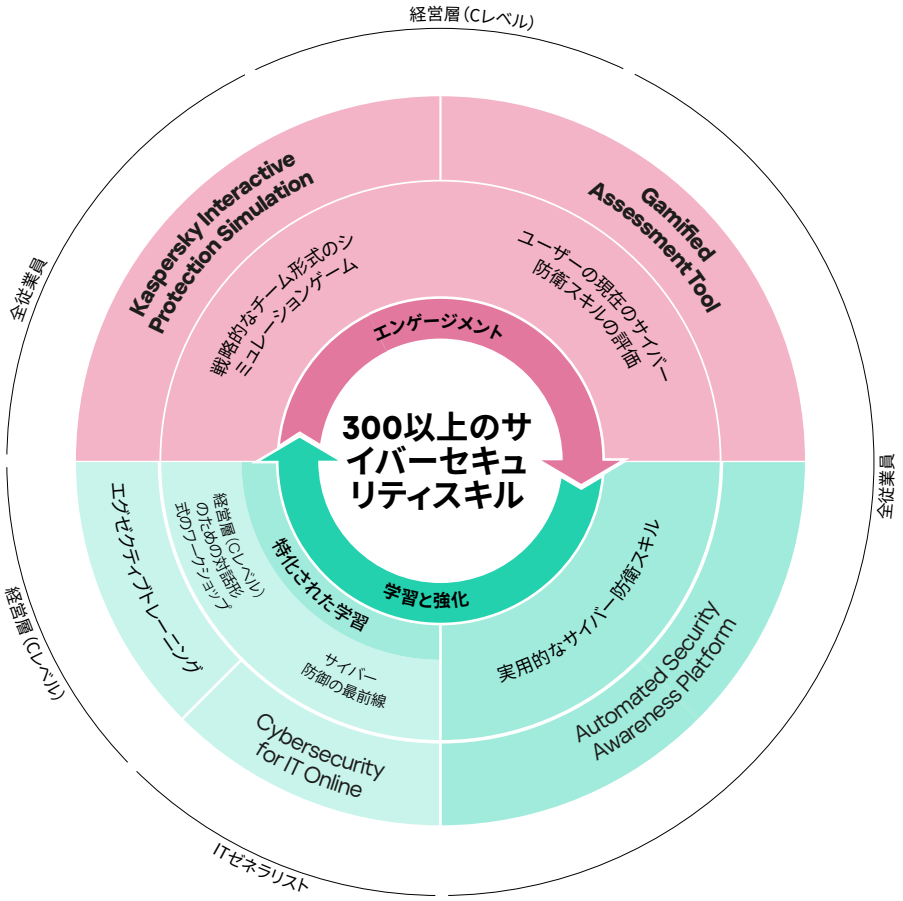
ASAPはKaspersky Security Awarenessポートフォリオの中核となる製品です。

すべての人に対応する単一のフレキシブルなソリューション

Kaspersky Security Awarenessには、長年にわたる世界的な実績があります。企業の規模を問わず、**75以上の国々の100万人を超える従業員の教育**に使用されているこのソリューションには、カスペルスキーが25年以上にわたって培ってきたサイバーセキュリティに関する経験と社会人向け教育の豊富な経験が活かされています。

このポートフォリオは、職位に関係なくあらゆる従業員が**サイバーセキュリティに対して高い意識を持つようになり**、組織全体のサイバーセキュリティに貢献できるようにする、幅広い魅力的なトレーニングオプションを提供します。

行動の変容には長い時間がかかります。そのため、複数の構成要素から成る継続的な学習サイクルを構築するアプローチがとられています。ゲームベースの学習に上級管理職も関与させて、彼らをサイバーセキュリティイニシアチブの支持者やサイバーセーフな行動をとる文化構築の支援者に変えます。ゲームを利用したアセスメントにより、従業員の知識のギャップを明確にし、さらなる学習へのモチベーションを高めることができ、オンラインプラットフォームとシミュレーションにより、従業員に正しいスキルを身につけさせ、強化することができます。



Kaspersky ASAPの無料トライアルはこちら： k-asap.com/ja
エンタープライズサイバーセキュリティ：www.kaspersky.co.jp/enterprise
Kaspersky Security Awareness：www.kaspersky.com/awareness
ITセキュリティニュース：blog.kaspersky.co.jp/category/business

www.kaspersky.co.jp

kaspersky bring on the future