全組織レベル向けのコンピューターベースのトレーニングプログラム

Kaspersky Security Awareness

kaspersky BRING ON THE FUTURE

詳しくはkaspersky.com/awareness をご覧ください

Kaspersky Security Awareness
組織全体の効果的なサイバーセキュリティ構築方法

サイバーインシデント（サイバー攻撃やIT環境上で発生する事故）の80%超は、人為的ミスによって引き起こされています。組織を通じてサイバーセキュリティを意識した行動をとり、基本的なサイバーセキュリティスキルと認識を高めることが、攻撃サーフェスを縮小して対応するインシデントを減らすための鍵となります。多くの場合に、従業員に適切な行動を教育する効果的なトレーニングのためのツールや手法を見つけるのは難しい課題です。このために重要なのが、成人向けの最新の教育手法や技術を使用し、最も関連性のある最新の教材を提供するトレーニングを実施することです。

ヒューマンファクターがサイバーセキュリティの最も脆弱な要素

サイバーセキュリティソリューションは急速な発展とともに複雑な脅威に適応し、サイバーセキュリティの最も脆弱な要素であるヒューマンファクターにつけ込もうとするサイバー犯罪者にとって攻めづらい標的となっています。

経営幹部の 52% は、従業員が運用上のセキュリティに対する最大の脅威であると言っています *

小企業の 43% が、従業員による IT セキュリティポリシー違反を原因とするセキュリティインシデントを経験しています **

従業員の 60% が会社所有のデバイスで機密データ（財務データ、メールデータベースなど）を有しています ***

従業員の 30% が
業務用 PC のログイン名とパスワードを同僚と共有していることを認めています ***

組織の 23% が企業データストレージにサイバーセキュリティルールやポリシーを設定していません ***

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

Kaspersky Security Awarenessは、従業員のサイバーセキュリティ意識を高め、全員が組織のサイバーセキュリティを向上させるための役割を担えるようにするための魅力的で効果的なトレーニングソリューションです。行動に変化をもたらすには長期間を要することから、複数の構成要素が含まれる継続的な学習サイクルの構築に関わるアプローチがとられています。

継続学習サイクル

エンゲージメント/モチベーション	スタート地点	学習	強化
– なぜ学習が必要か – 認識	– セキュリティについて十分な認識を持っているか – 何を学習すべきで、足りない知識は何か	– マイクロラーニング – 継続学習 – 適応力	– 正しく理解できたか – 学習内容を覚えているか – 学習内容に沿って対応しているか

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

20 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りました。

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、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。

* 「Weathering the Perfect Storm: Securing the Cyber-Physical Systems of Critical Infrastructure」レポート （2020年）

** レポート「IT security economics 2021」（カスペルスキー）

*** 「Sorting out a Digital Clutter」カスペルスキー、2019。

意欲的に学習してセキュリティ意識を効果的に高める

従業員のミスが経済的損害を被る企業

1,315,000 米ドル
大企業1社あたりの損害額
従業員の不適切な IT 資源利用によるデータ漏えいが及ぼす経済的影響の平均 *

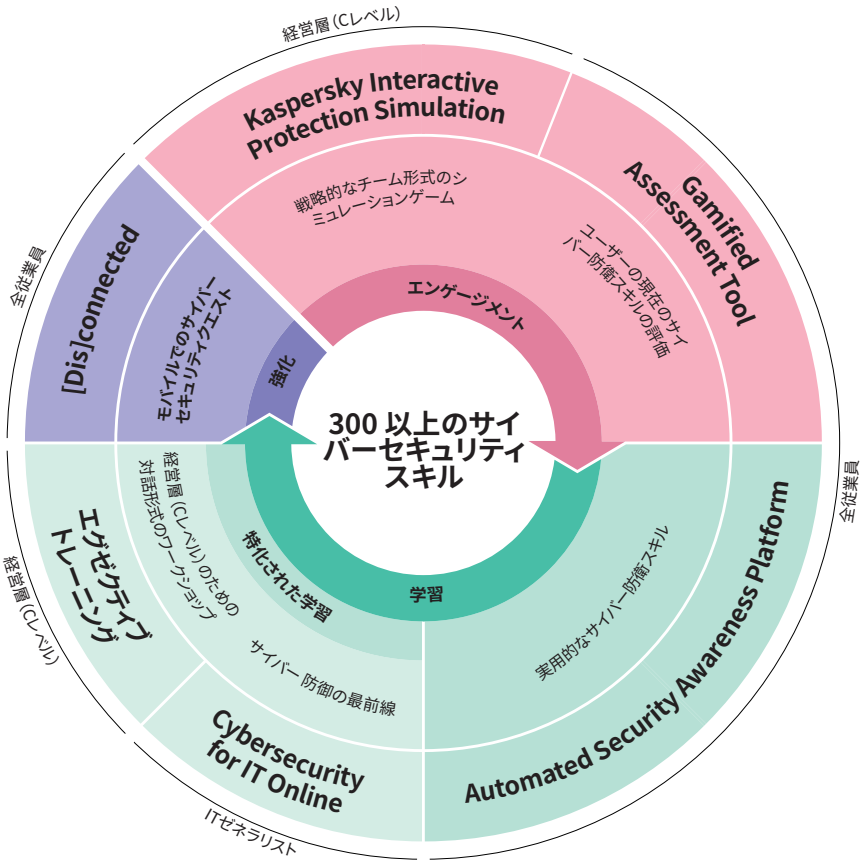
従業員の50% は
企業が
従業員の不適切な振る舞いを原因とする、直接的な脅威を経験しており、これが IT セキュリティのもっとも一般的な脅威となっています *

86%
企業が
少なくとも 1 人の社員がフィッシングリンクをクリックしたと主張しました **

501 万米ドル
(BEC 攻撃からの侵害 1 件にかかる平均的なコスト)
(BEC (Business Email Compromise) は、攻撃者が企業の正規のメールアカウントを乗っ取ったり、なりすましたりするフィッシング攻撃の一種です)

従業員の行動を変えることは、サイバーセキュリティの最大の課題です。人は一般的にスキルの獲得や習慣を変えることに意欲的でないので、多くの場合に教育活動は中身のない形式的なものに終わりがちです。効果的なトレーニングはさまざまな要素で構成され、人間の性質や獲得したスキルを吸収する能力が考慮されています。サイバーセキュリティのエキスパートであるカスペルスキーは、安全なユーザー行動がどのようなものかを熟知しています。その洞察と知識を活かし、お客様の従業員が攻撃への免疫を持ちながら、制約されることなく自由に活動できる学習手法を取り入れています。

さまざまな組織レベルに応じたトレーニング形式



* レポート「IT security economics 2021」（カスペルスキー）
** Cybersecurity threats trends 2021 (CISCO)
*** 「Cost of a Data Breach」 (2021)IBM

Kaspersky Security Awareness ソリューション

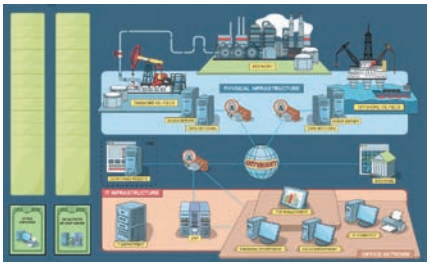
モチベーション

強制的なトレーニングには、従業員はあまり乗り気にはなりません。サイバーセキュリティは、複雑すぎるもの、退屈すぎるもの、自分とは関係のないものと考えられてしまう傾向があります。学習する意欲がないと、成果が身につくことは期待できません。教育プログラムの担当者にとってもう1つの課題がエグゼクティブ向けのトレーニングです。彼らの誤りは誰よりも大きな損害をもたらします。このために容易されたゲームトレーニングは大変魅力的で、トレーニングに抵抗を感じる人でも効果的に学習を行うことができます。

70%
の学習内容が
従来形式のトレーニングではその日のうちに忘れられてしまいます

42%の回答者(従業員1,000名以上の企業)が
参加したトレーニングプログラムの多くは役に立たず、つまらないと感じています**

KIPSトレーニングは上級管理職、ビジネスシステムエキスパート、ITプロフェッショナル向けに、あらゆるITシステムとプロセスに伴うリスクや課題についての意識を向上させるプログラムです。



Kaspersky Interactive Protection Simulation (KIPS)：ビジネス視点で見るサイバーセキュリティ

KIPSは2時間の対話式チームゲームで、意思決定者（上級管理職、IT/サイバーセキュリティ担当役員）が相互の理解を通じてサイバーセキュリティに対する認識を変えることを目的としています。マルウェアなどによる攻撃が実際に業績や収益に与える影響をソフトウェアでシミュレートします。プレーヤーは戦略的な思考で攻撃による影響を予測し、決められた時間とコストで適切に対応することが求められます。すべての判断があらゆるビジネスプロセスに影響する中で、円滑に運営を進めることが重要なゴールになります。ゲームを終了して最も収益をあげ、サイバーセキュリティシステムのすべての欠陥を見つけて分析し、適切に対処できたチームが勝利します。

業界に関連する 13 のシナリオ（随時追加予定）

それぞれのシナリオでは、新たな課題と脅威、組織がサイバーセキュリティを構築する時に犯す一般的な過ちにに注目しつつ、ビジネスの継続性と収益性の面におけるサイバーセキュリティの真の役割を説明しています。営業チームとセキュリティチームとの連携を高めることで安定した運営を維持し、サイバー脅威に対する持続性も得ることにもつながります。

シナリオのカスタマイズ

2022 年第 3 四半期から、選択した業界シナリオについて、企業はさまざまな攻撃を使った独自のゲームシナリオを作成できるようになります。さまざまな攻撃の組み合わせを使用することで、KIPS エンタープライズライセンスを持つ企業は、同じ業界シナリオを複数回実行できます。

KIPS Virtual Reality

KIPS Power Station VR では、発電所の実際の運用に可能な限り近い現実的な環境で新しい没入型体験を行えます。このテクノロジーにより、マネージャーは情報セキュリティスペシャリストとして「働く」ことができ、サイバーセキュリティの役割とそのビジネスへの影響を視覚的に示すことができるため、IT による決定がもたらす結果に関する抽象的な考えを持つだけではなく、非常にリアルな 3D グラフィックスでその結果を確認することができます。

スタート地点

自分の能力がどれほど不足しているかを意識せずにいることは、とりわけ脆弱さを招く要因となります。サイバーセキュリティ能力を試し、詳細で明確なフィードバックを得ることが、さらに効果的なトレーニングにつながります。既に熟知している内容のために時間を無駄にすることもありません。

Gamified Assessment Tool: 従業員のサイバーセキュリティスキルを簡単に楽しく評価

Kaspersky Gamified Assessment Tool（GAT）は、従業員のサイバーセキュリティに関する知識を簡単に知ることができます。楽しい対話形式で、従来の評価ツールにありがちな退屈さはありません。15 分の短い時間でサイバーセキュリティに関する 12 の日常シーンに答えながら、それがリスクを伴う行動であるか、確実な対応であるかを判断します。

完了すると発行される証明書には、スコアとサイバーセキュリティの認識レベルが記されます。すべてのゾーンについて、説明とヒントを含めたフィードバックが与えられます。

GAT のアプローチは意欲的に学習しながら、特定の状況を解決することで知識とのギャップを明らかにすることができます。IT/HR部門向けにも、組織のサイバーセキュリティ認識レベルを理解して、さらなる教育活動への導入として利用することができます。

学習

弊社のオンライン学習プラットフォームは、意識向上プログラムの中核です。すべての主要な IT セキュリティトピックをカバーする **300 以上のサイバーセキュリティスキル**を含みます。
レッスンごとに紹介される実例をもとに、日常業務の中で対処すべきことを身近に感じながら学ぶことができます。これらのスキルは、学んだ後にすぐに役立てることができます。

Kaspersky ASAP：従業員のサイバーセキュリティスキルを段階的に構築する、管理しやすいオンラインツール

ASAPで扱うトピック:

- パスワードとアカウント
- 電子メール
- 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
- PC セキュリティ
- モバイルデバイス
- 機密データの保護
- GDPR
- 産業向けサイバーセキュリティ

ASAP 速習コース

オーディオビデオ形式の短期トレーニングコース

- インタラクティブな理論
- ビデオ
- テスト

Kaspersky ASAP は多言語で提供されているソリューションです。

Kaspersky Automated Security Awareness Platform：あらゆる規模の組織のトレーニング管理の効率と容易さ

Kaspersky ASAP は従業員のサイバーセキュリティスキルを高めて意欲的に適切な行動をとれるようにするための効果的で使いやすいオンラインツールです。

トレーニングはすべての企業のセキュリティ意識のニーズを満たしますが、自動化された管理は、特に専用のトレーニング管理リソースを持たない企業にとって魅力的なものです。

主な利点

- **完全自動化されたシンプルなプログラム：**簡単に起動、設定してモニターできるプログラムです。その後の管理も完全に自動化されていて、管理者は必要ありません。プラットフォームがグループごとの教育スケジュールを設定するので、学習モジュール、メールによる学習強化、テストやフィッシング攻撃シミュレーションなど、さまざまなトレーニング形式により自動で定期的に学習が行えます。
- **効率的:** プログラムの内容は、常に学習を強化しながら段階的に学習を進められる構成がとられています。人の記憶に基づく方法論を通じて、確実に知識を維持してスキルの実践が図れます。
- **柔軟な学習：**自分に合った従業員トレーニングオプションを選択してください。サイバーセキュリティトレーニングの規制要件をすばやく満たしたり、従業員の知識を更新したりしたい場合は、基本的な速習コースを従業員に割り当ててください。また、より詳細で深いサイバーセキュリティスキルの開発を行いたい場合は、複雑さのレベルで細かく分類されたメインコースを選択してください。
- **柔軟なライセンス**（マネージドサービスプロバイダー向け）：5 つのライセンスから始められるユーザーごとのライセンスモデル。

ASAP は MSP および xSP に最適です– 複数の企業向けのトレーニングサービスを 1 つのアカウントで管理でき、毎月のライセンスサブスクリプションが使用できるようになっています。

Kaspersky ASAP の完全に機能が揃ったバージョンを asap.kaspersky.com で試し、独自の企業セキュリティ意識向上トレーニングプログラムの設定および管理の容易さをご自分でご確認ください！

メインコース

速習コース

強化

強化学習は、学習プログラムの重要な過程であり、学習で獲得した知識とスキルを定着させるために必要なものです。

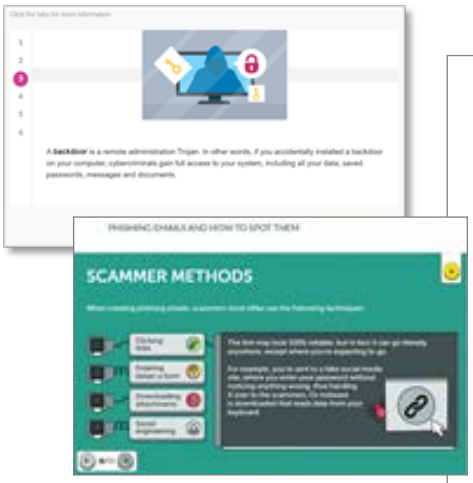
学んだスキルを習慣にする最良の方法は実践することです。同時に、人は誤りをし、自らの経験から学習をするものです。しかし、サイバーセキュリティに関しては、自身の誤りから学ぶことはひどくコストのかかる場合があります。

ゲームによるトレーニングは、自分や会社に何ら損害を与えることなく、危機的な状況とその結末を「体験」することができます。

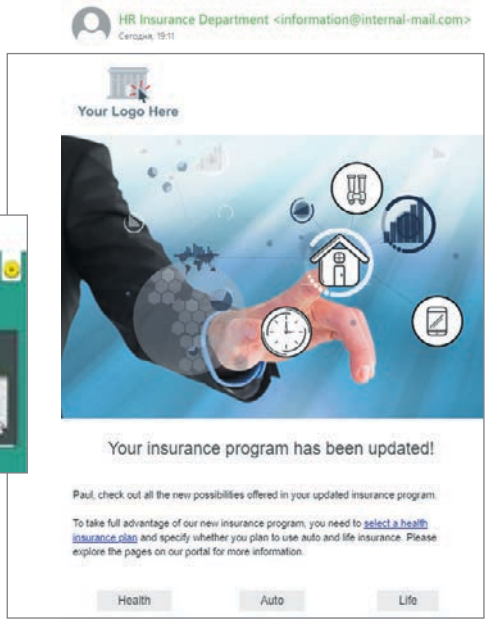
フィッシング攻撃シミュレーション

シミュレートされたフィッシング攻撃を、トレーニング前、トレーニング中、トレーニング後に使用して、サイバー攻撃に対抗する従業員の能力をテストして彼らを助けることができます。また、それによって会社の経営陣は、トレーニングのメリットを確認できます。

対話型のレッスン



フィッシング攻撃シミュレーション



結果の追跡

学習状況をダッシュボードから確認して、組織全体と全グループの進捗をひと目で把握できます。個々のレベルで詳細を掘り下げることもできます。

[Dis]connected：モバイルサイバーセキュリティクエスト

[Dis]connected は楽しいストーリーに富んだ、没入型のビジュアル体験ができるサイバーセキュリティゲームです。プレーヤーは健康なワークライフバランスを追求して、生活と仕事の両立を目指します。

サイバーセキュリティのさまざまな要素が織り込まれたシナリオをもとに、自分の判断がこれらの目標の達成（あるいは失敗）にどのように影響するかを知ることができます。パスワードとアカウント、メール、Webブラウジング、ソーシャルネットワークとメッセンジャー、コンピューターセキュリティとモバイルデバイスに関するトピックを含めた18の問題が用意されています。メッセンジャーやバンキングアプリなど、実際と同じアプリケーションを使うことで、没入感のあるゲームを楽しめます。

ゲームを終えると、プロジェクトがどれだけ成功したかが示され、現在と将来に向けて十分なセキュリティスキルがあるかを知ることができます。

ゲームは携帯電話でプレイできます。**無料デモ**は Google Play と App Storeで入手できます。
https://kas.pr/mobilestores

高度な学習

一般的な IT スペシャリスト：標準的な意識向上プログラムは、ヘルプデスクやその他の技術に精通した社員にとって不十分なものであるため、彼らはトレーニングから除外されることがよくあります。しかし、企業は彼らをサイバーセキュリティの専門家に変える必要もありません。専門家の育成は、非常に高価で、時間を要する、不要なものです。

このギャップを埋めるトレーニングを発表できることを嬉しく思います。専門家向けのトレーニングほど詳細なものではありませんが、一般の従業員向けのトレーニングよりも高度なものとなっています。

CITO トレーニングモジュール：

- 悪意のあるソフトウェア
- 不要である可能性のあるプログラムやファイル
- 調査の基礎
- フィッシングインシデント対応
- サーバーのセキュリティ
- Active Directory のセキュリティ

CITO の配信方法：
クラウドまたは SCORM 形式

CITO モジュールの 1 つを無料でお試しください。 cito-training.com

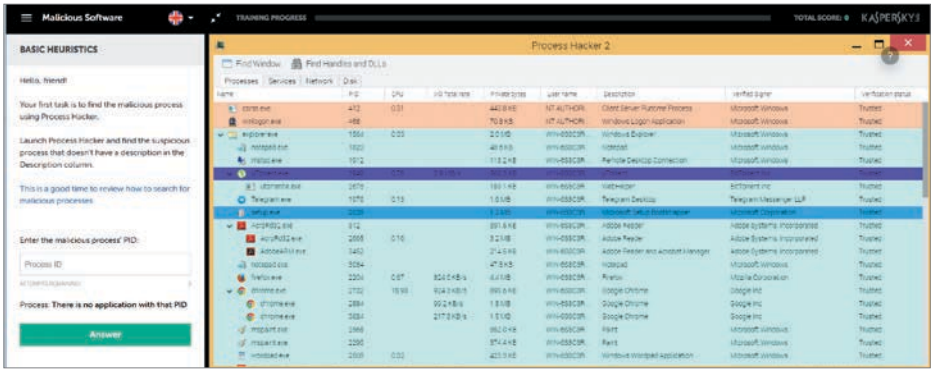
Cybersecurity for IT Online：最前線のインシデント防御

Cybersecurity for IT Online は、IT に携わるあらゆる従業員向けの対話式トレーニングです。サイバーセキュリティと第一線のインシデントレスポンスに関する高度なスキルを習得できます。

このプログラムにより、IT の専門家は、表面的には問題のない PC インシデントで発生する可能性のある攻撃シナリオを認識するための実践的なスキルを身につけることができます。悪意のみられる兆候を積極的に見つけることで、ITチームの全メンバーがセキュリティ防御の第一線を担う役割を獲得できます。

また、CITO では、調査の基本と IT セキュリティツールおよびソフトウェアの使用方法を学べるようになっており、IT プの専門家は理論的なスキル、実践的なスキル、および演習ベースのスキルを身に付けて、IT セキュリティに引き継ぐためのインシデントデータを収集できるようになります。

組織のすべてのITスペシャリスト向けに推奨されるトレーニングですが、主にサービスデスクとシステム管理者を対象としています。エキスパート以外のITセキュリティチームメンバーにも役に立つコース内容です。



経営陣はサイバー犯罪者にとって最も望ましいターゲットの 1 つですが、教育者にとっては本当に難しい課題となることがよくあります。しかし、さまざまなサイバーセキュリティへの取り組みや支援に対して彼らの関与やサポートがなければ、組織内にサイバーセーフティ文化を構築することは不可能です。

サイバーセキュリティは、プロジェクト管理、金融商品、および事業運営の効率性とともに、収益創出における重要な側面であります。これが経営者向けのコースの中心となる事柄です。

エグゼクティブトレーニング：デジタル変革のための企業の回復力の向上

企業のリーダーや経営陣は、チューターによるコースを通じてサイバーセキュリティの基本を学び、サイバー脅威とそれらから保護する方法について理解を深めることができます。

調査によると、インシデント対応の速度や効率と、インシデントがもたらしうる損害の程度との間には直接的な関係があります。このコースでは、サイバーセキュリティの財務的側面とそれへの投資の実現可能性に特に注意を払い、経営幹部がサイバーセキュリティとビジネス効率の関係に関する理解を深められるようにします。

実践的な演習を行い、より統合された教材を提供するために、このトレーニングに加えて、Kaspersky Interactive Protection Simulation (KIPS) を使用する場合があります。

コースの目的

- 現代のサイバー脅威とそのビジネスへのリスクに関する最新情報を共有する
- 学習者に最新のサイバー脅威の状況を知らせる
- 企業および個人のサイバーセキュリティ文化の基本的なルールを実践する機会を提供する
- 情報セキュリティの分野における主要な規制問題のビジネスへの影響を学習者が理解しているを確認する
- サイバーセキュリティの基本的な概念と、標的型攻撃からの保護方法を明確にする
- 企業の方針に関する実践的な推奨事項を提供する
- インシデントへの対応と調査のためのコミュニケーションに関するアドバイスを行う

Kaspersky Security Awareness：柔軟なトレーニング方法

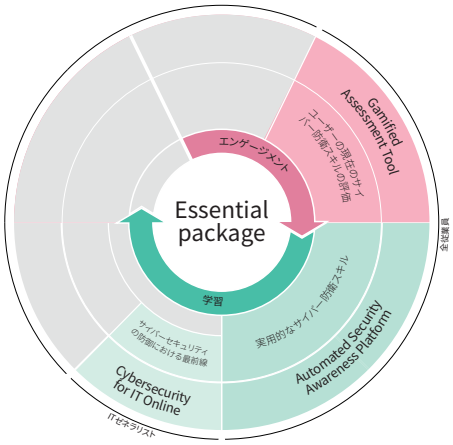
カスペルスキーのトレーニングソリューションは、企業のあらゆるレベルをカバーしており、単独またはまとめて使用することができます。
また、貴社のニーズに合わせたパッケージを簡単に使い始められるようにしています。

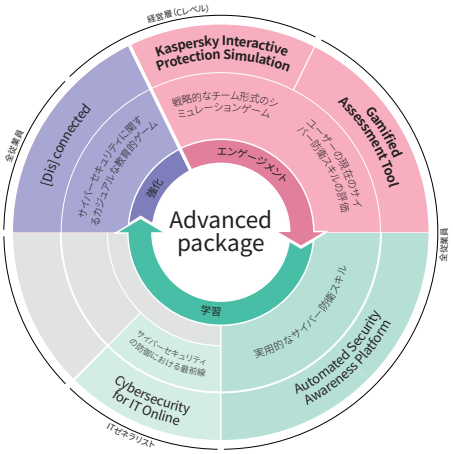
手間を掛けずに、サイバーセキュリティに関する従業員の意識を向上 – セットアップはシンプル、管理は簡単

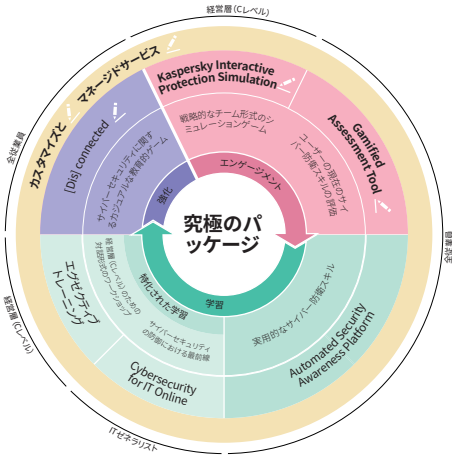
基本レベルのセキュリティトレーニングを提供して、貴社が正常な組織運営をし、一般的なサイバーセキュリティトレーニングの規制またはサードパーティの要件を満たせるようにします。

大規模な組織がシンプルな「ターンキー」トレーニングソリューションを使用して、ビジネスの継続性を維持できるようにします。学習サイクルのすべての段階をカバーすることにより、すべての組織レベルをサポートし、行動を変えます。

カスタマイズとマネージドサービスを備えた最大限のサイバーセキュリティ意識を確保し、経営者が脅威シナリオに精通し、従業員が自動的にサイバーセーフスキルを身に付け、ジェネラリスト IT スタッフが防御の最前線として貴社をサポートできるようにします。







Kaspersky Security Awareness トレーニングは、最新のトレーニング方法と高度な技術を使用して、成功を確実にします。
柔軟な新しいパッケージソリューションはニーズに合わせて調整できるため、万人向けのソリューションがあります。
詳しくは kaspersky.com/awareness をご覧ください。

Kaspersky Security Awareness：kaspersky.com/awareness
ITセキュリティニュース：kaspersky.co.jp/category/business

kaspersky.co.jp

© 2022 AO Kaspersky Lab.
All rights reserved.
登録商標およびサービスマークは
それぞれの所有者に帰属します。

kaspersky BRING ON THE FUTURE