あらゆる職位の従業員のためのサイバーセキュリティスキル

Kaspersky Security Awareness

kaspersky bring on the future

詳しくはこちら：
kaspersky.co.jp/awareness

Kaspersky Security Awareness
組織全体でサイバーセーフティの文化を構築

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。組織全体でサイバーセキュリティを意識した行動をとる文化を構築し、基本的なサイバーセキュリティスキルと意識を高めることが、攻撃サーフェスを縮小して対応すべきインシデントを減らすための鍵となります。社会人教育の最新の技術とテクノロジーを採り入れたトレーニングを行い、関連性が高い最新のコンテンツを提供することこそが、行動変容を成し遂げて「人的要因」に起因するサイバーセキュリティの問題を解消する最善の方法です。

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を遂げ、複雑な脅威に適応しており、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を追い詰めています。

55%の企業が、自社従業員によるITセキュリティポリシー違反を報告*

43%の中小企業が、従業員の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報告**

データ漏えいはセキュリティに関する最も一般的な問題であり、**最も一般的な原因は従業員**（22%）と攻撃者（23%）。*

30%の従業員が業務用PCのログイン名とパスワードを同僚と共有***

23%の組織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ない***

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、長年にわたって世界的な実績を誇る効率的なソリューションです。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。

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。

継続学習サイクル

1 → 2 → 3 → 4

1 エンゲージメント/モチベーション
- なぜ学習が必要か
- 認識

2 スタート地点
- 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

3 学習
- マイクロラーニング
- 継続学習
- 適応力

4 整理
- 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

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。

* 「IT Security Economics 2022」カスペルスキー

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

*** 「Sorting out a Digital Clutter（デジタルクラッターの分類）」、カスペルスキー、2019年

意欲的に学習してセキュリティ意識を効果的に高める

従業員のミスが企業に経済的損害を与える

$52.887
大企業1社あたりの損害額
従業員の不適切なIT資源利用によるサイバー攻撃の被害額*

30%
のマルウェア侵害
偽のリンクや添付ファイル付きのメールを介して実行されるマルウェア侵害**

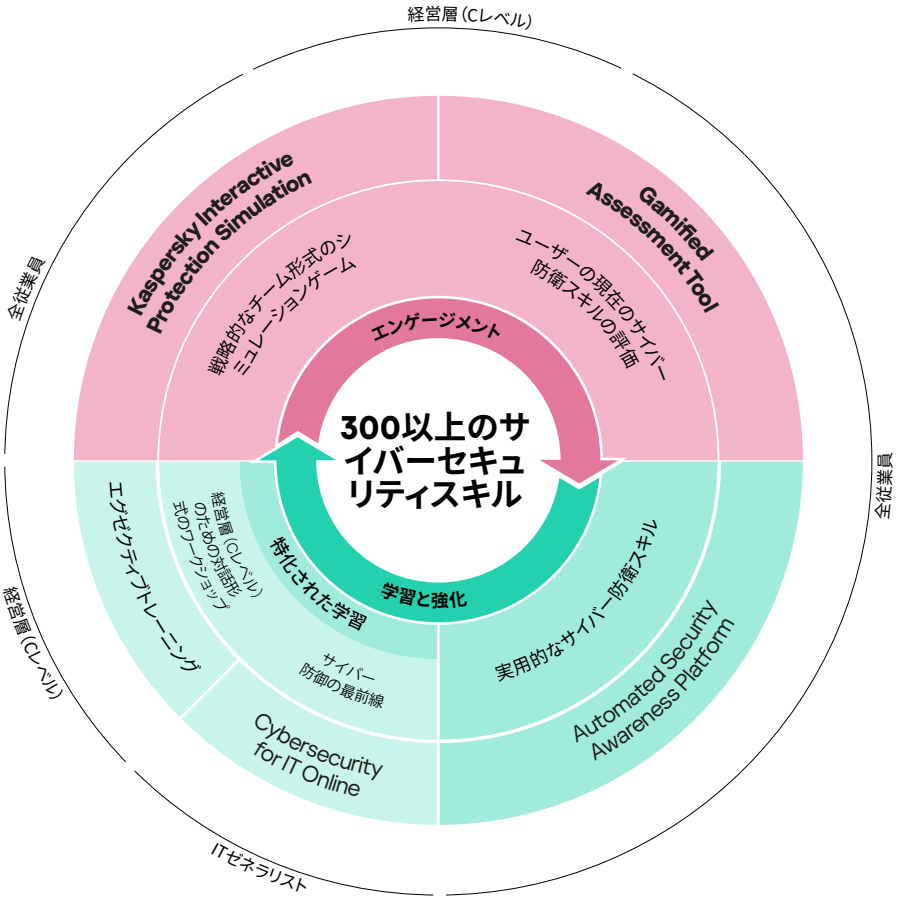
79%
の従業員
過去1年間に、リスクを認識しているにもかかわらず、リスクのある行動を少なくとも1回したと回答した従業員***

$164
レコード1件あたり被害額
レコード数2,200～102,000件の侵害による全世界での平均被害額****

42%の回答者
（従業員1,000名以上の企業）
参加したトレーニングプログラムの多くは役に立たず、つまらなかったと回答*****

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



* 「IT Security Economics 2022」カスペルスキー
** 「Data Breach Investigation Report」（2022）
*** 「Balancing Risk, Productivity, and Security」、Delinea（2021）
**** 「Cost of a Data Breach」 （2022)IBM
***** Capgemini、「The digital talent gap」

Kaspersky Security Awarenessソリューション

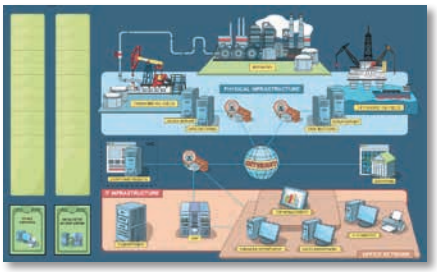
エンゲージメントとモチベーション

強制的なトレーニングに従業員は得てして気が進まないものです。サイバーセキュリティは複雑すぎる、退屈すぎる、自分とは関係のない、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。このために用意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。

76%のCEOが、業務スピードを上げるためにセキュリティプロトコルを回避し、セキュリティを犠牲にしていることを認めています*。

62%の管理職が、組織内でのITセキュリティに関するコミュニケーション不足が、1件以上のサイバーセキュリティインシデントにつながったと認めています**。

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ションします。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。

2つのKIPSオプション

人気の高いKIPS Liveオプションは、オンサイトで実際に対面して競い合うことで、興奮と熱狂の雰囲気を作り出します。従業員が積極的に参加して組織内にサイバーセキュリティのカルチャーを構築できるようにする役に立つツールです。

KIPS Onlineバージョンでは、プレイヤーはどこからでも参加でき、他の多くの参加者と対話できます。KIPS Onlineはグローバルな組織や公的な活動に最適です。さらに KIPS Liveと組み合わせることで、オンサイトイベントにリモートチームを参加させることもできます。

- 最大300チーム（=1000人のメンバー）が同時に、どこからでも参加できます。
- チームごとに別言語のゲームインターフェイスを選択できます。
- プリインストールされているシナリオを、参加人数や用途に合わせてカスタマイズできます。ライブラリから、ゲーム上で発生する攻撃の回数と種類を選択できます。
- また、オンラインバージョンのメリットとして、プレイヤーが何を選択したかの統計情報や、特定状況下におけるチームの行動に関するデータ、前のゲームと比較したプレイヤーの行動に対するベンチマークを参照することができます。

大企業向けのKIPS

ライセンス期間中何度でもKIPSをプレイできるライセンスをお持ちのお客様は、あらかじめ設定された内容でプレイすることも、ライブラリからさまざまな攻撃を選んで組み合わせ、プレイするたびにゲームシナリオをパーソナライズすることもできます。この機能により、毎回ゲームに変化が生まれ、より面白いものになります。

---

* https://www.forbes.com/sites/louiscolumbus/2020/05/29/cybersecuritysgreatest-insider-threat-is-in-thec-suite/?sh=466624f87626

** https://www.kaspersky.com/blog/speak-fluent-infosec-2023/

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）により、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てい 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のアプローチにより、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のギャップを特定できます。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

カスペルスキー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。主要なITセキュリティトピックをすべてカバーする**300以上のサイバーセキュリティスキル**が含まれています。
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、学んだ後すぐに役立てることができます。

Kaspersky Automated Security Awareness Platform：あらゆる規模の組織のトレーニング管理をより容易で効率的に

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、管理の自動化が可能なことは、専任のトレーニング管理リソースを持たない企業にとってとりわけ役に立ちます。

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ます。その後の管理も完全に自動化されているため、管理者 による作業 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、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。
- **管理者にとっての使いやすさ：**プラットフォームの自動管理、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）、ユーザーフレンドリーなダッシュボード、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。
- **学習者にとっての使いやすさ：**明確なレッスン構成、実際の業務に即した例、ユーザーフレンドリーなインターフェイス、メールのリマインダー、必要に応じて別のレッスンに戻ってやり直す機能、PCやモバイルに対応するインターフェイスなど、すべてが学習プロセスを楽しくて興味深く効果的なものにします。

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
- 個人情報
- 銀行キャッシュカードのセキュリティとPCI DSS
- ドクシング
- 暗号通貨のセキュリティ
- リモートワーク時の情報セキュリティ
- ロシア連邦法152-FZ

ASAPエクスプレスコース

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
- 動画
- 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。

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のすべての機能を asap.kaspersky.comでお試しください。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・管理がいかに容易なのかをご自分でお確かめください！

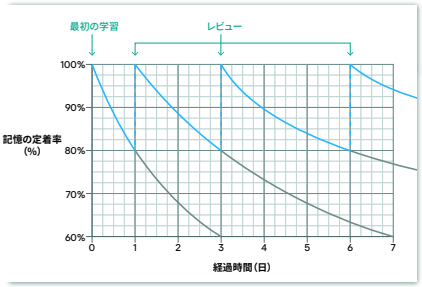
整理

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。

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



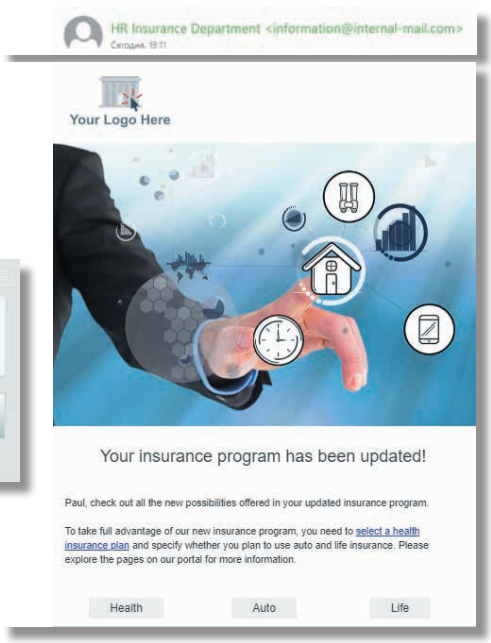
- **学習効率を考えられた構成：**プログラムの内容は、常に学習を強化しながら段階的に学習を進められる構成がとられています。人の記憶に基づく方法論を通じて、確実に知識を維持してスキルの実践が図れます。
- **カスタマイズ：**トレーニングプログラムの外観を簡単に変更して、管理者・学習者用のポータルやプラットフォームからのメールに表示されるカスペルスキーロゴを自社のロゴに変更したり、認定証をカスタマイズしたり、レッスンに個人的なコンテンツを追加したりできます。
- **学習の柔軟性：**自分に合った従業員トレーニングオプションを選択できます。サイバーセキュリティトレーニングの規制要件をすばやく満たしたり、従業員の知識を更新したりしたい場合は、基本的なエクスプレスコースを従業員に割り当てます。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、複雑さに基づいて細かく分類されたメインコースを選択してください。
- **ライセンスの柔軟性：**（マネージドサービスプロバイダー向け）：5件のライセンスから始められるユーザー単位のライセンスモデルです。1つのアカウントで複数の企業を管理できます。

フィッシング攻撃シミュレーション

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使用して、サイバー攻撃に対する従業員の対応能力をテストして従業員をサポートできます。これにより、経営陣はトレーニングのメリットを確認できます。

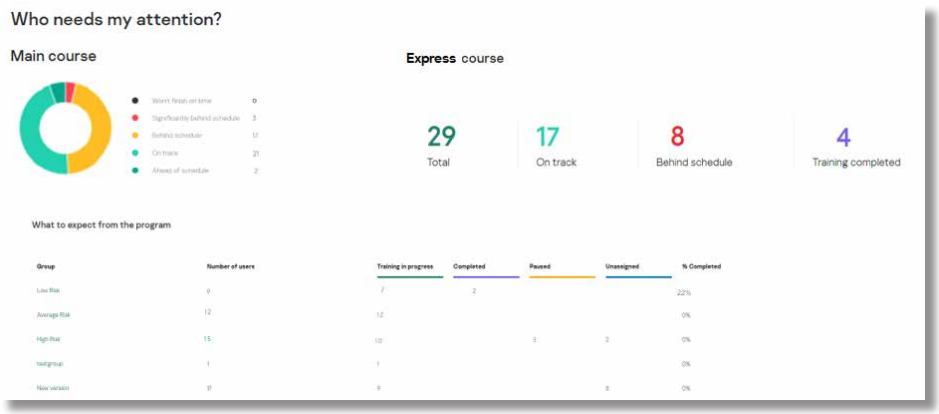
対話型のレッスン

フィッシング攻撃シミュレーション



結果をトラッキング

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。



特化された学習

ITゼネラリスト：ヘルプデスクやその他の技術に精通した社員にとって、標準的な意識向上プログラムは十分な内容ではないため、彼らはしばしばトレーニングから除外されます。しかし、こうした社員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。育成には非常に時間とお金がかかるうえ必要のないものものだからです。

そこでカスペルスキーは、このギャップを埋めるトレーニングを発表します。専門家向けのトレーニングほど詳細ではありませんが、一般の従業員向けのトレーニングよりも高度な内容です。

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

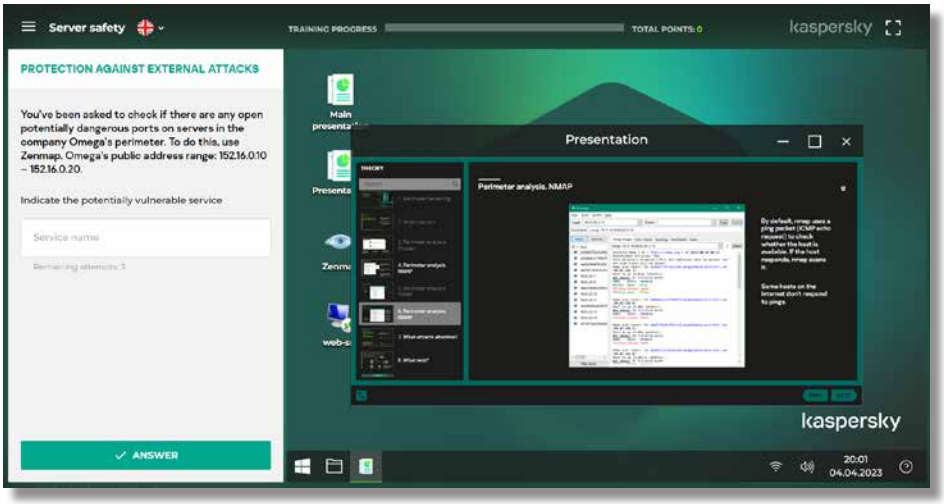
Cybersecurity for IT Online：最前線のインシデント防御

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。悪意の見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担当者は理論的なスキル、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セキュリティチームに引き継ぐ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。



経営幹部を関与させる

経営陣はサイバー犯罪者にとって理想的な標的の1つですが、教育者にとっては本当に難しい課題となりがちです。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の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す。これが経営幹部向けのコースの中心となるトピックです。

エグゼクティブトレーニング：

エグゼクティブトレーニング プログラムでは、ビジネスリーダーや経営幹部がチューターによる対話形式のワークショップやオンラインコースを通じてサイバーセキュリティの基本を学びます。サイバー脅威について理解を深め、脅威に対する防衛方法を把握することができます。

このコースでは、サイバーセキュリティの財務的側面とサイバーセキュリティへの投資の実現可能性に注目し、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ついて理解を深められるようにします。現在の脅威ランドスケープが自社に与える影響やサイバー攻撃の発生時にとるべき対策のほか、面白くて関連性の高い役に立つ情報が満載です。

KIPSトレーニングと組み合わせると、このコースをさらに活用できるようになります。企業ごとのセキュリティ啓発アプローチに応じて、KIPSをプレイする前でも後でも、エグゼクティブトレーニングを自由にご利用いただけます。

* 最新のモジュールリストはこちら：
cito-training.com

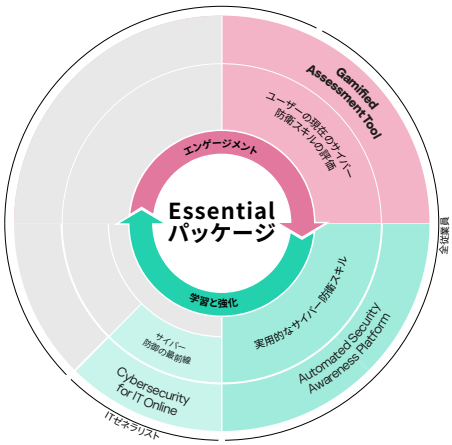
Kaspersky Security Awareness：柔軟なトレーニング方法

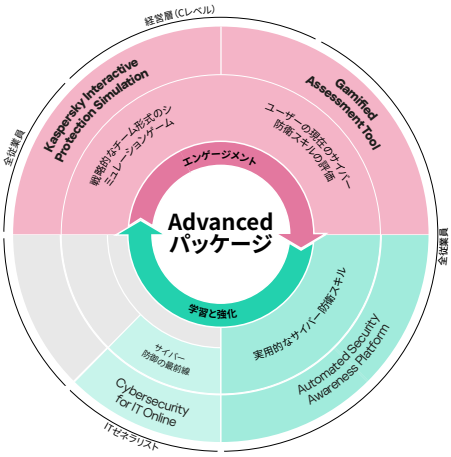
カスペルスキーのトレーニングソリューションは企業のあらゆるレベルをカバーしており、単独で使用することもまとめて使用することもできます。また、貴社のニーズに合わせて調整されたパッケージで簡単に使用を開始できます。

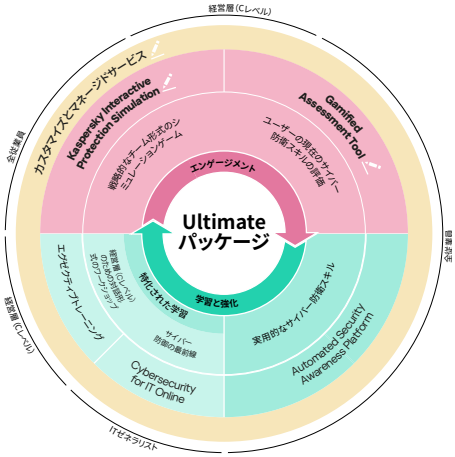
手間を掛けずに、サイバーセキュリティに関する従業員の意識を向上 – セットアップはシンプル、管理は簡単。
基本レベルのセキュリティトレーニングを提供して、企業が正常に組織を運営し、サイバーセキュリティトレーニングの規制要件またはサードパーティ要件を満たせるようにします。

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支援します。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が特長の、サイバーセキュリティに対する意識を大きく向上させるパッケージです。経営幹部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、ITゼネラリスト防御の最前線として会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により、成功を確実なものにします。柔軟な新しいパッケージソリューションをニーズに合わせて調整できるため、あらゆる状況に応じたソリューションが必ず見つかります。詳しくはこちらをご覧ください：kaspersky.co.jp/awareness

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

kaspersky.co.jp

kaspersky