Kaspersky Interactive Protection Simulation

経営幹部など意思決定者のサイバーセキュリティ意識を高める

kaspersky bring on the future

詳しくはこちら：
kaspersky.com/awareness

Kaspersky Interactive Protection Simulation

「人の問題」

今日、企業が直面しているセキュリティ上の最大の問題の一つは、上級管理職にあるような意思決定者たちが、サイバーセキュリティに対してポジションごとに異なる視点を持ち、その優先順位もばらばらであることです。その結果、意思決定過程にある種の「セキュリティバミューダトライアングル」が発生する可能性があります。

- 経営幹部は、セキュリティ対策がビジネス目標
- （経費削減、迅速化、品質向上）に反すると考える。
- IT セキュリティマネージャーは、サイバーセキュリティをインフラや投資の問題と考え、自分の管轄外として考慮しない可能性がある。
- コスト管理マネージャーは、サイバーセキュリティの支出が収益につながるものであり、コストを生み出すのではなく抑制するとは考えない可能性がある。

効果的なサイバーセキュリティを実現するためには、これら 3 者の相互理解と連携が不可欠です。しかし、従来型の啓発を促す講義やレッド/ブルーチーム形式の演習は、長いうえに専門用語が多く、忙しい管理職には不向きであり、「共通言語」を構築できないという欠陥があります。

企業のサイバーセキュリティは C レベルの幹部から始まる

今日、多くの企業にとって、IT インフラの持続可能性は優先事項の一つになっています。しかし、サイバーセキュリティの課題については、IT 担当者や IT セキュリティ担当者の責任と考えられることが多く、企業内部においてサイバーセキュリティ対策は一部でのみ重視されがちです。ビジネスリーダーは、主として売上、カスタマーエクスペリエンス、リスク、コストに集中しています。このような目標達成に取り組む中で、サイバーセキュリティが軽視されるのは珍しいことではありません。しかし、模範を示す取締役会のサポートがなければ、サイバーセキュリティのカルチャーを企業全体で構築することは、実際のところ難しいのです。

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**。

51% の情報セキュリティ担当者が、IT セキュリティの予算増額について話すことは非常に難しいと感じています。ところが、実行可能なコミュニケーション戦略については、意見が一致しています。

多くの C レベル幹部 **(56%) と IT 担当者 (48%)** が、IT セキュリティ関連の問題を円滑に伝えるには、実例を示すことが最も効率的であると考えています**。

Kaspersky Security Awareness の効果

Kaspersky Security Awareness は、長年にわたって世界的な実績を誇る効率的かつ効果的なソリューションです。**75 以上の国々のさまざまな規模の企業により 100 万人以上の従業員**を教育するために使用されているこのソリューションは、サイバーセキュリティにおける 25 年以上に及ぶカスペルスキーの経験と、社会人向け教育における Kaspersky Academy の豊富な経験に基づいて構築されています。

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、魅力的なトレーニング製品で構成されています。

ポートフォリオ内の各製品は、学習サイクル全体の中で個々の役割を果たしますが、単独でも利用可能です。

エグゼクティブのための戦略的サイバーセキュリティビジネスゲーム

Kaspersky Interactive Protection Simulation (KIPS) は、戦略的ビジネスシミュレーションとして、業務の効率性とサイバーセキュリティとの関係を実証するチームゲームになっています。

参加者は、IT セキュリティチームのメンバーとしてビジネス模擬環境に置かれ、会社を円滑に運営し利益を上げようとする中で、予期せぬサイバー脅威に次々と直面することになります。

参加者は、事前対策と事後対応の中から最適なものを選択し、サイバー防衛戦略を構築する必要があります。選択するたびに、シナリオの展開が変わり、これらが最終的に会社の収益に影響します。

チームは、エンジニアリング、ビジネス、およびセキュリティの優先順位を、現実的なサイバー攻撃にかかるコストに照らしてバランスを取りながら、データを分析し、不確実な情報と限られたリソースに基づいて戦略的な意思決定を行います。これらすべてのシナリオは現実に起こった出来事に基づいています。

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

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

KIPS は「プレイしながら学ぶ」ダイナミック意識向上ゲーム：

- 楽しく、魅力的で、あっという間（2 時間）
- 共同作業でチームワークを育成
- チーム間の競争を通じて分析スキルが向上
- ゲームを通してサイバーセキュリティ対策を理解
- すべてのシナリオとサイバー攻撃は事例に基づいている

KIPS の効果

KIPS トレーニングは、業務システムの専門家、IT 担当者、部門長を対象に、コンピューター化された現代のシステムの運用に伴うリスクやセキュリティ問題に対する認識を高めることを目的としています。

1 チーム 4〜6 名で、生産設備とそれを制御するコンピューターを含む事業を運営します。ゲーム中、生産設備により、売上、社会的認知度、さらにビジネス上の成果が生み出されます。同時にチームは、業績に影響を及ぼす恐れのあるサイバー攻撃に対処しなければなりません。

ゲームが終わると、プレイヤーは、自分の仕事に活かせる重要で実用的な洞察を得ることができます。

- サイバー攻撃は収益を直撃するので、経営幹部が対処すべき問題である
- あらゆる事業において効果的なサイバーセキュリティを実現するには、IT 部門とそれ以外の部門の意思決定者間の連携が欠かせない
- 適切なセキュリティ予算は高額にならないが、サイバー攻撃が成功した場合に失われる収益は多大である
- 従業員はセキュリティ管理にすぐに慣れ、その重要性を理解する（監査トレーニング、アンチウイルスなど）

2 つの KIPS オプション

人気の高い **KIPS Live** オプションは、興奮と熱狂の雰囲気を作り出し、サイバーセキュリティのカルチャーを構築するための素晴らしいツールとなっています。

KIPS Online バージョンでは、プレイヤーは各自都合の良い場所から参加でき、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ができます。

- 最大 300 チーム（=1000 人のメンバー）が同時に、どの場所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。
- 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できますし、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。
- 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。

KIPS により、以下のことを学ぶことができます。

- サイバーセキュリティが事業継続性と収益性に果たす役割。
- 企業が直面する新たな課題と脅威。
- 企業がサイバーセキュリティを確立する際に犯しがちな過ち。
- 業務チームとセキュリティチームの連携により、安定した事業運営とサイバー脅威に対する持続的な保護を実現する方法。

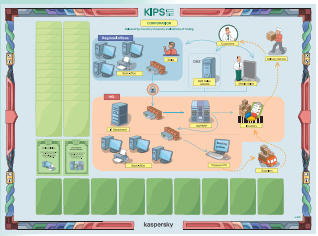
シナリオに応じて、各チームは特定業種の企業の IT セキュリティに責任を持ちます。チームメンバーの任務は、会社業務が正常に中断なく実行されるようにし、顧客やサプライヤーとの関係を良好に保ち、サイバー脅威を発見し無力化することです。

企業がサイバー攻撃を受けることで、プレイヤーは生産と収益への影響を経験します。そして、利益を失うことなく攻撃の影響を最小限に抑えるために、さまざまなビジネス戦略や IT 戦略、ソリューションを活用することを学びます。

ゲームが終了したとき、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落とし穴を見つけて分析し、適切に対処できたチームが**勝利します。**

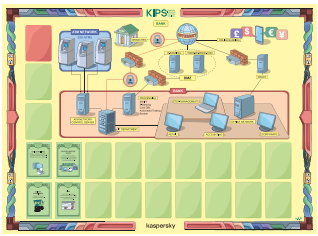
あらゆる業種における エンタープライズ KIPS シナリオ

一般企業



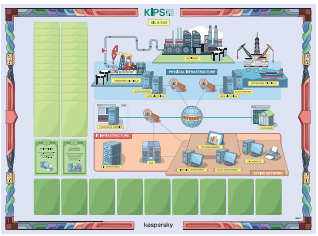
ランサムウェア、APT、オートメーションセキュリティの欠陥から企業を守る。

銀行



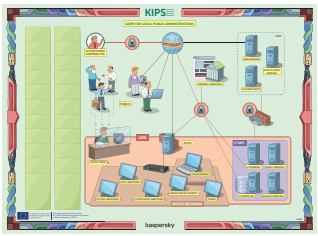
Tyukpin や Carbanak といった高レベルの APT から金融機関を守る。

石油ガス



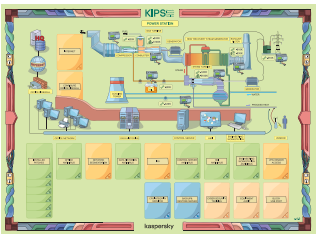
Web サイトの改ざんから本物のランサムウェア、高度な APT まで、さまざまな脅威の影響を探る。

自治体



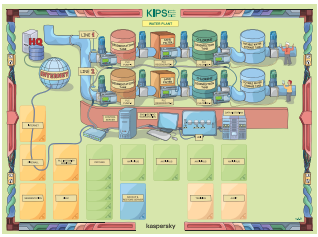
公開されている Web サーバーを攻撃や悪用から守る。

発電所



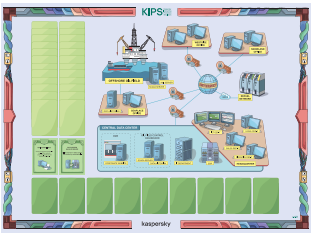
産業用制御システムと重要インフラを Stuxnet タイプのサイバー攻撃から守る。

浄水場



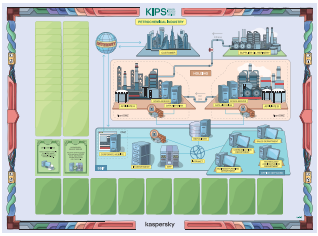
浄水場の IT インフラを守り、2 つの生産ラインの安定性を確保する。

石油販売



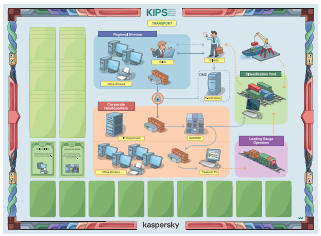
世界中に拠点を持つグローバルな石油・エネルギー企業の収益を守るために、サイバーセキュリティを確立する。

石油化学



エチレン生産に特化した大規模な石油化学ホールディングスの新しい支社が正常に機能するようにする。

運輸・交通システム

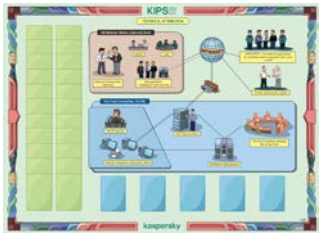


物流企業を **Heartbleed、APT、B2B ランサムウェア、内部者から守る。**

航空

空港で乗客の安全や荷物のタイムリーな到着を実現し、数々のサイバー攻撃や脅威から空港の資産を守る。

技術的なアトリビューション



国連のサーバーに対する複雑な APT 攻撃の調査および技術的なアトリビューションを行う。

中小企業

DDoS、ランサムウェア、モバイルアプリのハッキング、なりすましなどのサイバーセキュリティ脅威から中小企業の事業を守る。

電気通信業

通信事業者、クラウドサービスプロバイダー、ゲーム開発会社、本社からなる大手電気通信ホールディングスの資産を守る。

KIPS をさらに活用するには

KIPS の後は、Kaspersky Security Awareness ポートフォリオに含まれる**エグゼクティブトレーニング**をおすすめします。この管理職向けトレーニングは、KIPS をプレイする前でも後でも、企業ごとのセキュリティ啓発アプローチに応じてご利用いただくことができます。現在の脅威の状況や、サイバー攻撃の際に取るべき行動、その他興味深い情報や関連する有益な情報を知ることで、KIPS の体験をより深めることができます（エグゼクティブトレーニングには、インタラクティブなオフラインワークショップとオンラインコースの 2 つの形式があります）。

ゲームに関する KIPS ユーザーやお客様の声

Kaspersky Industrial Protection Simulation は本当に驚きの体験で、すべてのセキュリティ専門家に必須とされるべきものだと思います。

Warwick Ashford 氏
Computer Weekly

CERN には、膨大な数の IT システムとエンジニアリングシステムがあり、何千人もの人々がそれらのシステムを使っています。そのため、サイバーセキュリティの観点から、社員全員のサイバーセキュリティに対する意識を高めることは、技術的なコントロールと同じくらい重要なのですが、そんな当社にとって、カスペルスキーのトレーニングは、面白くて取り組みやすく、効率的であることが実証されました。

Stefan Luders 氏
CERN CISO

本当に目から鱗が落ちるような体験で、参加者からは「このゲームを会社で使ってみたい」という声が続出しました。

Joe Weiss 氏 PE,
CISM, CRISC, ISA Fellow

私たちは、提携や 協力に基づく人々のネットワークを構築しなければなりません。KIPS は、それを実現できるパーフェクトな方法です。

Daniel P. Bagge 氏
Národní centrum kybernetické bezpeč nosti, Chezh Republic

KIPS セッションの準備

スケジュール：KIPS を 1 つの独立したイベントとして計画するか、既存のイベント/カンファレンス/セミナー内の 1 つのセッションとして計画します（後者の場合、初日の最終時間帯が KIPS 実施に最適な時間帯になります）。

グループ：20〜100 名を 3〜4 名のチームに分けます。各チームに、経営者、エンジニア、CISO/IT セキュリティ担当者が含まれている構成が理想です。
- 各役割/職務から最低 1 名は参加するのがベストです。
- チームは、同じ会社/部門どうしの構成にすることもできますし、異なる会社/部門が混ざる構成にすることも可能です。
- 参加者が顔見知りであるかどうかは問題にはなりません。

セットアップ：ゲームの所要時間は 1.5〜2 時間ですが、準備とセットアップのために、ゲームの 2 時間前にはカスペルスキーのファシリテーターチームが部屋を利用できるようにしておく必要があります。

部屋：3 m2 以上/人、柱なし、標準的な AV 機器： プロジェクター（6〜8 ルーメン）、スクリーン、音響システム（スピーカー、リモコン、マイク）。

Wi-Fi 4 Mbps 以上の インターネット環境（KIPS ゲームサーバーへのアクセス用）、Wi-Fi 対応 iPad を各チーム（4 名）ごとに用意するか、その他のタブレットを用意する。

机・椅子：
参加者用テーブル 4 人分（長方形: 75×180 cm 以上、円形: 直径 1.5m 以下）、参加者は 4 人 1 組でテーブルに座ってください。共同主催者用のテーブル、参加者全員用の椅子。

参考情報と事例紹介

これまでに 50 か国以上の産業セキュリティ分野の専門家が KIPS Game をプレイしています。

- KIPSは、英語、ロシア語、ドイツ語、フランス語、日本語、スペイン語EU、スペイン語LA、ポルトガル語、トルコ語、イタリア語、中国語、オランダ語、アラビア語に翻訳されています
- KIPS は、Cyber Security Malaysia、チェコ共和国の NSA、オランダの Cyber Security Centrum など、多くの政府機関で使用されており、国の重要インフラ組織における何百人もの専門家の危機意識を高めています
- SANS Institute などの主要教育機関が KIPS のライセンスを取得し、世界中の SANS 受講生向けのトレーニングで KIPS が使用されています
- 三菱日立パワーシステムズなどのベンダーやセキュリティサービスプロバイダーが KIPS のライセンスを取得し、重要インフラ顧客向けのトレーニングで KIPS が使用されています
- KIPS は、欧州委員会の Geiger プロジェクトの一環として、中小企業や零細企業をサイバー脅威から守り、プライバシー管理を向上させるためのトレーニングとして使用されています

トレーナーの育成が可能

お客様が KIPS を使用して、より幅広い対象者（複数の部門や拠点にいる多数の社員、マネージャー、専門家）にトレーニングを提供する必要がある場合、KIPS トレーニング用のライセンスをご購入いただけます。これにより、社内トレーナーを育成して、お客様に都合の良いペースで KIPS セッションを実施できるようになります。

このタイプのライセンスには以下が含まれます。

- KIPS トレーニングプログラムを社内で使用する権利。
- トレーニング教材一式およびその使用権と再作成権。
- ライセンス期間中の KIPS ソフトウェアサーバーに対するログイン名/パスワード。
- トレーナーズガイド、および KIPSトレーニングの実施方法に関するプログラムリーダー向けの教育とトレーニング。
- メンテナンスとサポート（KIPS ソフトウェアとトレーニングコンテンツのアップデートとサポート）。
- （オプション）KIPS シナリオのカスタマイズ（別途料金がかかります）。

パートナーおよびトレーニングセンター向け KIPS

KIPS は、パートナーにとって、意識向上ソリューションをさまざまな形で活用できる絶好の機会です。製品として販売できるだけでなく、トレーニングセンターの顧客に販売したり、自身でセッションを実施したりできます（パートナーがこのオプションを選択した場合、カスペルスキーのトレーニングスペシャリストが、トレーナーとしてのパートナーのスキルアップをサポートします。）

Kaspersky Security Awareness

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

行動に変化をもたらすには長期間を要することから、複数の構成要素を含めた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は、上級管理職を巻き込み、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。

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。

継続学習サイクル

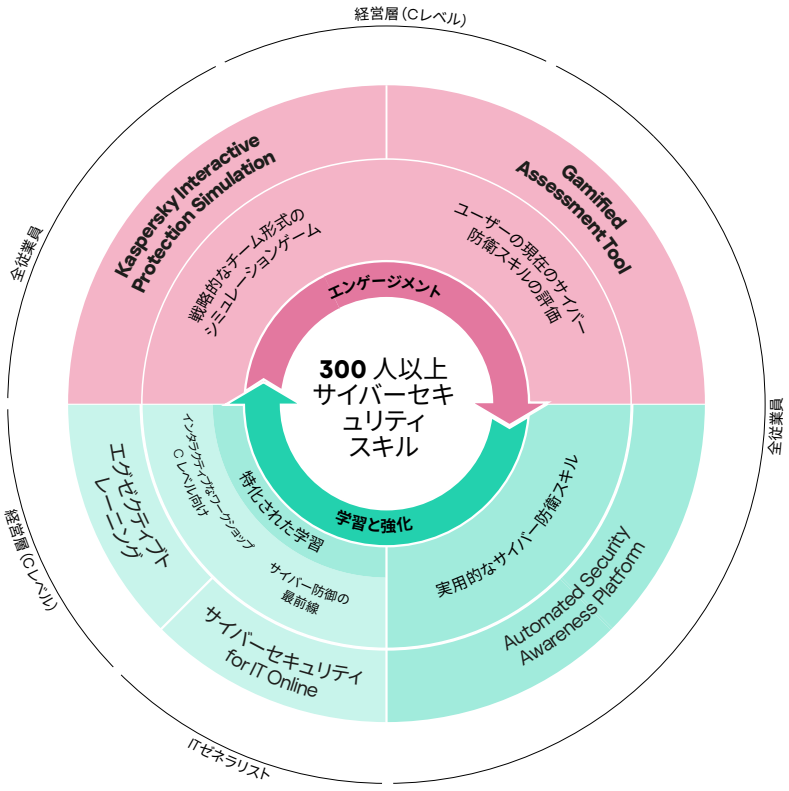
エンゲージメント/モチベーション
- なぜ学習が必要か
- 認識

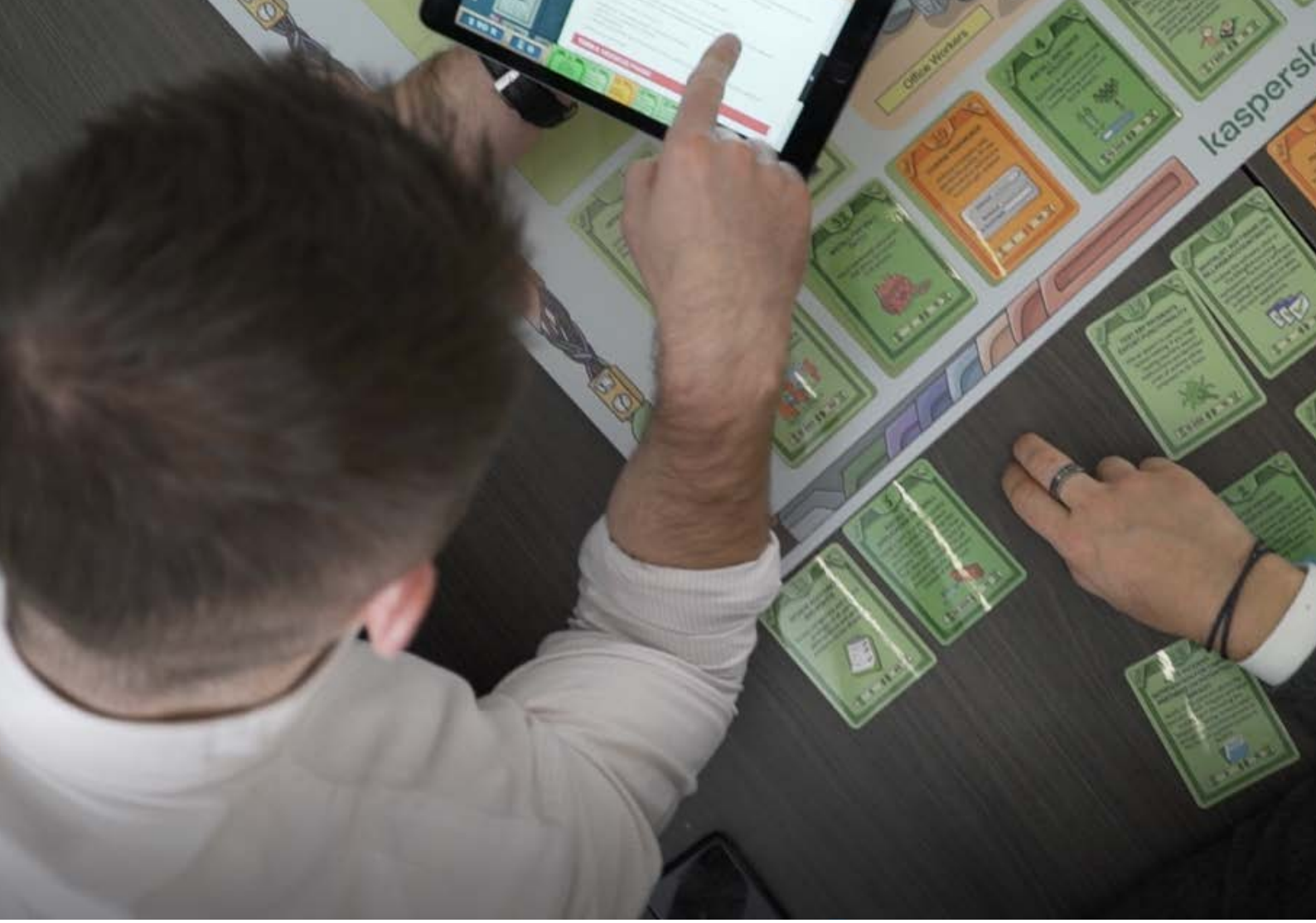
スタート地点
- セキュリティについて十分な認識を持っているか
- 何を学習すべきで、足りない知識は何か

学習
- マイクロラーニング
- 継続学習
- 適応力

強化
- 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

さまざまな組織レベルに応じたトレーニング形式





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

www.kaspersky.co.jp

kaspersky