



**Kaspersky
Security
Awareness**

kaspersky.co.jp



Gamified Assessment Tool

kaspersky bring on
the future



**Kaspersky
Gamified Assessment
Tool**

Gamified Assessment Tool

Kaspersky Gamified Assessment Tool (GAT) : 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

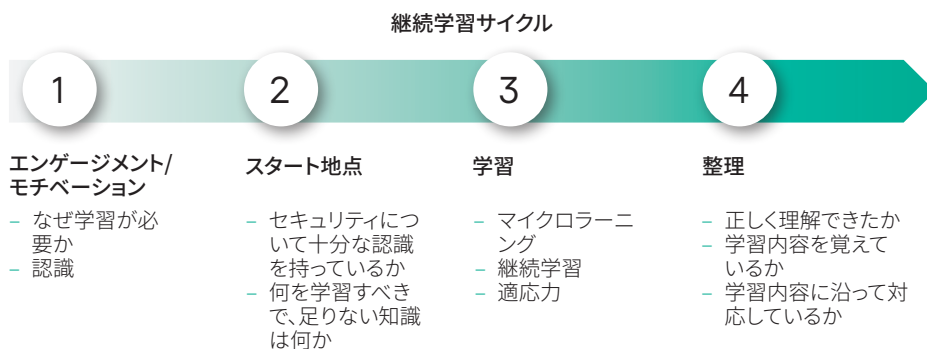
52%の大企業と50%の中小企業で、従業員の不適切なIT資源の利用によるサイバーセキュリティインシデントが発生*

42%の企業が、ITセキュリティに関する最大の懸念事項は従業員であると回答 (ITリソースの不適切な使用、企業所有のデバイスの紛失、フィッシングやソーシャルエンジニアリング攻撃の被害)*

119万5,000ドル: 従業員の不適切なIT資源利用によるデータ漏えいの経済的影響の平均*

現在、多くの企業で、強力なサイバーセキュリティが最も重要な課題となっていますが、これは手が回っていない領域でもあります。世界中の企業がサイバーセキュリティに熱心に取り組み、ますます複雑で効率的な保護システムの開発を進めています。それにもかかわらず、どの企業のサイバーセキュリティ環境にも、技術的な手法では埋められない穴が残っています。

このギャップこそが、「人的要因」です。人的要因は、サイバーセキュリティインシデントの主な原因の1つとなっています。従業員の行動を変えるのは難しい課題です。従業員はサイバーセキュリティを学ぶことに興味がありません。やる気がなく、多くの場合は自分の知識にギャップがあることに気づいてさえいません。どうすれば従業員にトレーニングを受けたいと思ってもらえるのでしょうか？サイバーセキュリティの現在の知識レベルを評価する方法は？Gamified Assessment Toolなら、従業員の現在のサイバーセキュリティスキルのレベルを測定し、もっと学びたいと思ってもらえます。CIOやHR部門は、ゲーム化された短いツールを教育プログラムの導入部として使い、会社のサイバーセキュリティ意識の全体像を把握することができます。



Gamified Assessment Toolの機能

- 評価には、オープンスペースでの仕事、移動中の仕事、在宅中の仕事という3つのシナリオがあり、特定のサイバーセキュリティスキルを必要とする一般的な状況が描かれています。
- それぞれの従業員に、特定のサイバーセキュリティスキルを必要とする12のランダムな状況から成るシナリオが提示されます。従業員は、登場人物の行動が危険かどうかを評価し、回答にどれくらい自信があるかをチップを使って表しながら、最後までシナリオを完了する必要があります。それぞれの回答で特定のポイントが加算されます。ユーザーの最終スコアの計算では、回答が正しいかどうかと自信度が考慮されます。
- 不正行為を予防し、評価をもっと楽しくするために、従業員に提供されるシナリオはランダムに決まります。それぞれのシナリオを構成する12の状況も、225種類の状況が含まれるライブラリからランダムに選ばれます。つまり、ユーザーによって評価のシナリオが違うということです。
- ユーザーがすべてのゾーンを完了すると、サイバーセキュリティ意識レベルを評価した総合スコアが表示されます。さらに、各ゾーンに関するフィードバックが、解説と役に立つヒントとともに表示されます。
- 評価が完了すると、認定証が付与され、ダウンロードしてシェアできます。
- 評価の管理者には、すべてのユーザーのレポートが、各トピックの詳細な結果 (スコア、正解数、自信度など) 付きで提供されます。従業員のサイバーセキュリティ能力のレベルについてのわかりやすくフィードバックを参考に、今後のセキュリティ意識トレーニングの計画と設定をより効果的に進められます。

* レポート: 「IT security economics in 2019 (2019年ITセキュリティの経済)」、カスペルスキー

Gamified Assessment Toolで扱うセキュリティ領域

- パスワードとアカウント
- 電子メール
- Webの閲覧
- ソーシャルネットワークとメッセージャー
- PCセキュリティ
- モバイルデバイス

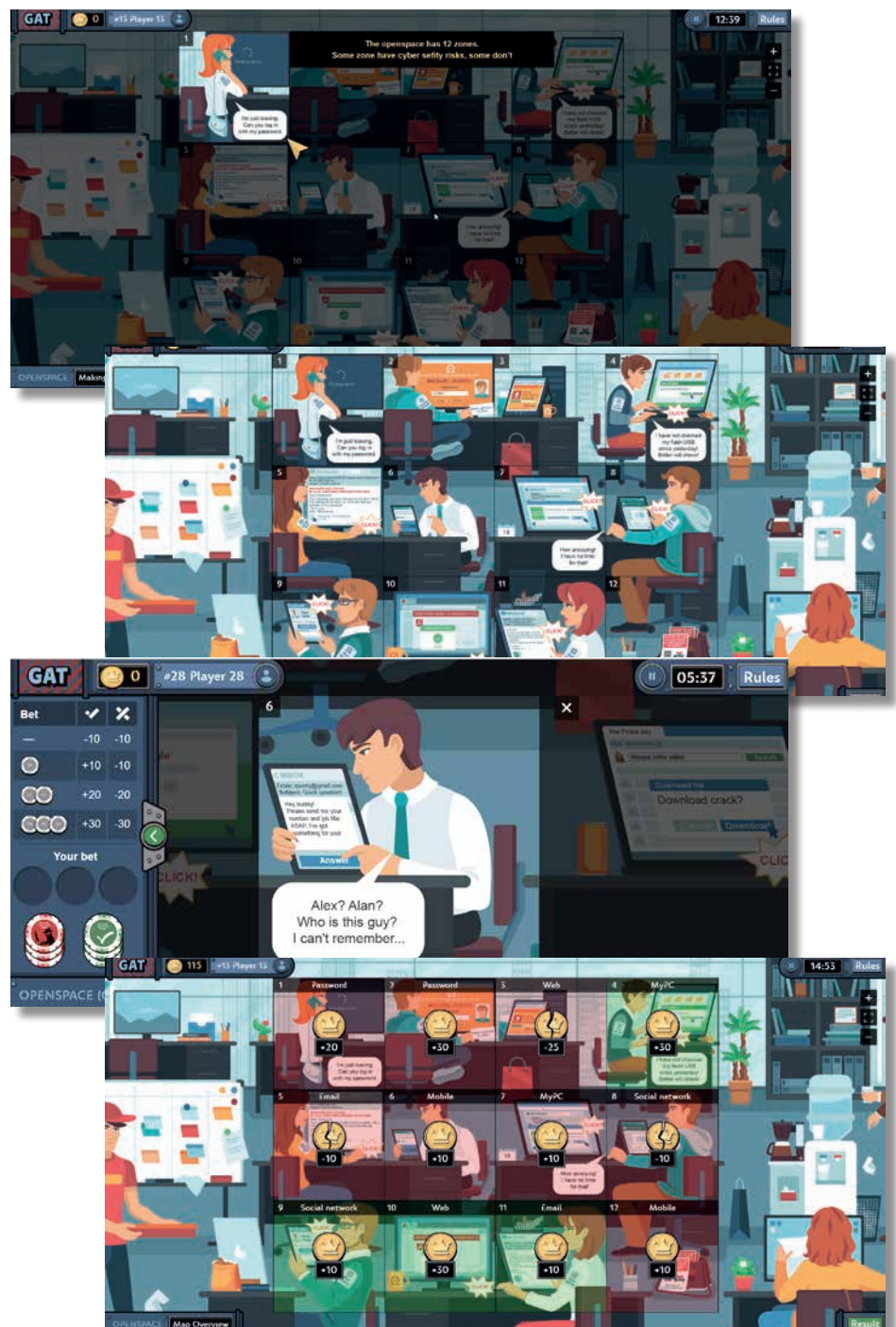
学習プロセス

評価は、ルールについての簡単な説明から始まります。

従業員は10分以内に、シナリオで描かれているサイバーセキュリティ関連の12の状況で登場人物がとる行動について評価する必要があります。この評価では、登場人物の行動が危険なものかどうかを判断し、回答にどれくらい自信があるかも答えます。ゲーム内では一時停止が可能です。別の用事がある場合、忘れずにゲームを一時停止してください（一時停止ボタンは、右上隅のタイマーの近くにあります）。

ユーザーは、危険ではないと思う場合は**緑色のチップ**を、危険だと思う場合は**赤いチップ**を置きます。チップの枚数は、回答にどれくらい自信があるかを表します。

ユーザーがゲームを終えると、サイバーセキュリティ意識レベルの評価が総合スコアとして表示されます。



それぞれの状況を見直すこともできます。

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受けられます。

評価の最後に、結果が記された認定証が提供されます。これには、特に注意を要するサイバーセキュリティピックや改善点についての推奨事項、今後のセキュリティ意識トレーニングのヒントも記されています。ダウンロードしてシェアできます。

技術上の推奨

OS:

Windows 7, 10

Mac: Sierra, High

Sierra, Mojave, Catalina

Ubuntu 18.04

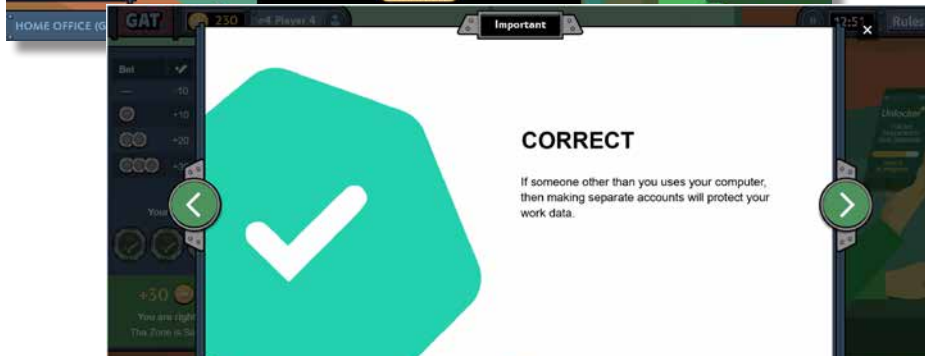
以下のブラウザの利用を推奨:

Firefox 70以降

Chrome 80以降

Safari 11以降

クラウドソリューションであるGATは、デスクトップブラウザまたは解像度が1024x768以上のタブレットPCのみを必要とします。



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をもとに、製品の中核となるスキルセットを構築



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

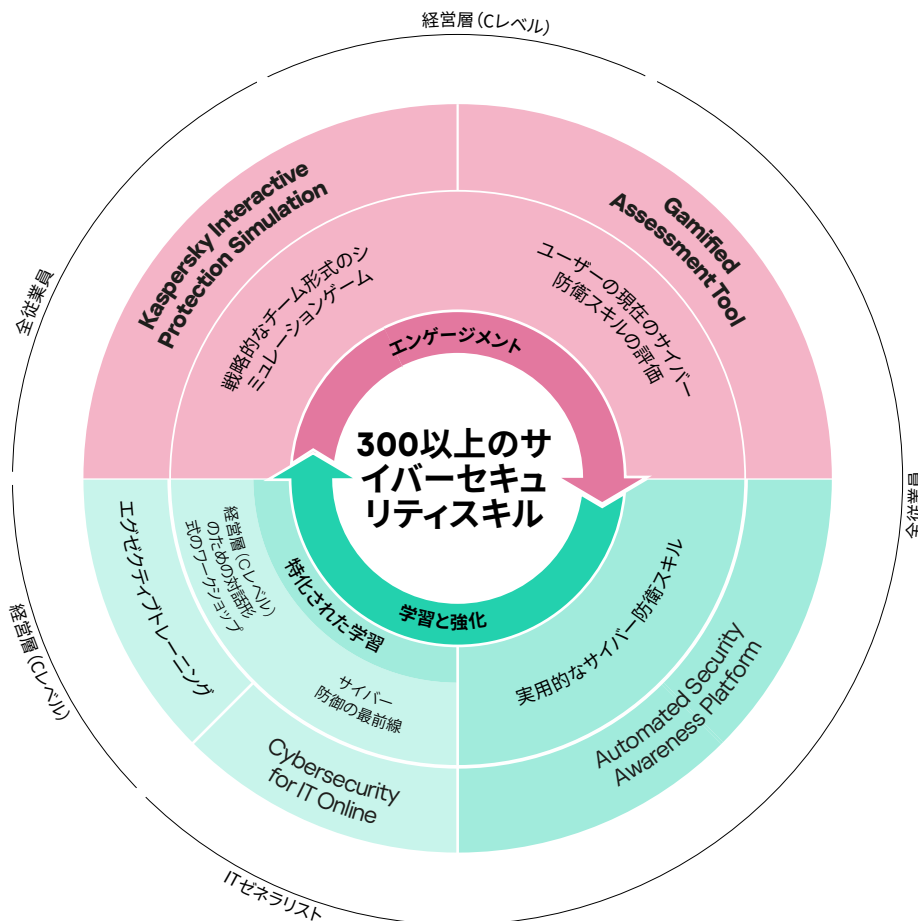
ゲーム形式のトレーニングはエデュテインメントを活用した、学習意欲のわく内容で、学習プラットフォームを通じて、サイバーセキュリティスキルを吸収でき、学んだスキルを長く記憶することができます。

すべての人が使える、単一のフレキシブルなソリューション

Kaspersky Security Awarenessには、長期にわたって国際的に成功を収めてきた実績があります。**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オプションで構成されています。

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。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。



Kaspersky ASAP の無料トライアルはこちら：k-asap.com
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