Kaspersky Security Awareness

組織の防御力を底上げするためのゲーム形式のトレーニングプログラム

www.kaspersky.co.jp
#truecybersecurity

組織全体でサイバーセーフティを実現するための効果的な方法

サイバーインシデントの 80 % 以上は人為的ミスによるものです。つまり、従業員に起因するインシデントから復旧するために、大企業は数百万ドルを失っています。そして、このような問題の防止を目的に開発された従来のトレーニングプログラムは効果が限られ、従業員は本質的な課題を理解することなく、組織が目指すべきサイバーセキュリティを実現できずにいます。

従業員の不注意が、組織で発生するサイバーセキュリティインシデントの原因の大部分を占めます。

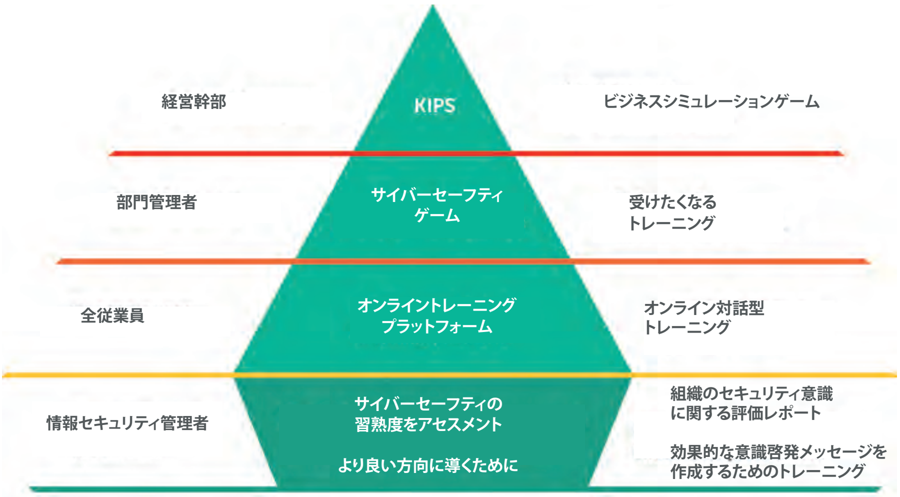
- IBM の 2015 年の報告によると、**人為的ミスに起因するインシデントの割合は 95 % を超えています**[1]。
- 2015 年においては、**英国の大規模組織の 75 %** および小規模事業者の 31 % **が、従業員に起因するセキュリティ侵害の被害を受けています**[2]。
- 従業員の不注意なミスに起因するインシデントの**平均的な経済的影響は、1件につき 865,000 ドル**[3]に達します。
- **年間の従業員あたりのフィッシング攻撃による平均損失額は最大 400 ドルに達します**（その他のサイバー脅威は除外）[4]。
- 人為的ミス、誤り、および不注意に起因するインシデントのうち保険で補填されるのは、**サイバー保険のうちのわずか 25 %** であると報告されています（一方、社外のサイバー犯罪者に起因するリスクでは 84 % が補填されており、悪意があるかインサイダーに起因するサイバー犯罪リスクでは全体の 75 % が補填されているという報告があります）[5]。

分析の結果、既存のサイバーセキュリティ意識向上トレーニングプログラムの多くは効果がないことが示されています。

- サイバーセキュリティポリシーと行動規範の解説だけでは退屈で、専門用語や技術に詳しくないければ十分な理解が得られません。
- 受講者の多くは学習する意欲を持つことなくトレーニングを終えます（犯罪者のターゲットになる可能性があると確信するのはわずか 22 %）。
- 受講者である従業員にとって、IT セキュリティは業務を妨げるだけで、ビジネスを助けてくれるパートナーであるとは考えていません。
- 「トレーニングを修了した人数」以外には、効果測定の指標になるものがありません。

プログラムの利点

Kaspersky Lab は、最新の学習手法を用いて組織のさまざまなレベルに対応したコンピューターベースのトレーニングプログラムを提供しています。



Kaspersky Security Awareness は、企業の目的と優先事項に合うように設計されています：

- **適切な行動を促し、一般的な座学以上の効果を提供：**学習手法には、ゲーミフィケーション、実践的学習、模擬攻撃などが含まれます。受講者が積極的に参加し自発的に学習することで、効果は長期間持続します。
- **異なる組織レベルに適したトレーニングを提供：**経営幹部、部門管理者、一般従業員の各レベルに対応しています。
- **効果測定と管理が容易：**実績のある体系的なトレーニングのベストプラクティスを提供するだけでなく、情報セキュリティ部門または人事部門による管理が可能です。
- ベースとなるのは膨大な **Kaspersky Lab のサイバーセキュリティ基盤と高度な調査研究能力**

1 IBM 2015 サイバー・セキュリティー・インテリジェンスの指標

2 2015 Information Security Breaches Survey（情報セキュリティ侵害に関する調査）。英国政府と InfoSecurity Europe および PwC が共同で実施

3『Business Perception of IT Security:In The Face of an Inevitable Compromise』、Kaspersky Lab、2016 年

4 Ponemon Institute による試算、『Cost of Phishing and Value of Employee Training』、2015 年 8 月

5 2015 Global Cyber Impact Report。Ponemon Institute LLC

ビジネス戦略をシミュレーションする KIPS（サイバー演習）

KIPS の対象者は経営者を含む経営幹部、部門管理者、および情報セキュリティ管理者であり、稼働中の最新のコンピューターシステムに関するリスクとサイバーセキュリティ上の問題の分析スキルを向上させることが目的のチーム戦形式のサイバー演習です。

Kaspersky Interactive Protection Simulation（KIPS）は、一連の予期しないサイバー脅威に晒されたときに、利益を最大限に保護し、信頼を維持することを目的とした演習です。その狙いは、あらかじめ用意されたサイバーセキュリティ対策の中から最適な選択することにより、サイバー防衛戦略を立案し、実施することです。

次々に発生するセキュリティイベントへの対処方法に応じて、その後のシナリオの展開および企業の最終的な利益または損失の程度が変化します。各チームは、サイバー攻撃の被害に対するエンジニアリング、ビジネス、およびセキュリティの各優先事項を考慮して状況を分析し、不確実な情報と限られた予算や実施可能な対策に基づいて戦略的な意思決定を行います。各シナリオはチームが置かれた状況で変化するセキュリティイベントに基づいて決定されているため、実際にサイバーインシデントが発生した状況をシミュレーションするだけでなく、適切な戦略に基づいた意思決定と、選択された対策の有効性をリアルタイムに検証することができます。

KIPS は、次の特徴を持つ「ゲーミフィケーション」を基にしたサイバー演習です：

- ゲーム形式で楽しみながら集中して短時間で完了（2 時間）
- 共同作業により、組織の垣根を越えて協調性が高まる
- リアルなセキュリティイベントを追体験することで、自主性と分析スキルを育成

「ただし、演習から得られる成果は、セキュリティ監査とトレーニング、パスワード変更、パッチ管理などの最も基本的で重要ないくつかの戦略的意思決定です。これは、以後実施する必要があるインシデント対応において非常に有効です。」

Mark Jenkins 氏　2015 年 12 月 16 日　ICT Qatar

利用可能ななシナリオ（10か国語に対応）

企業版・運輸版	ランサムウェア、APT、オートメーションセキュリティの不具合から企業を保護
銀行版	APTによる攻撃や、ATM、管理サーバー、ビジネスシステムへの攻撃から金融機関を保護
自治体版	脆弱性攻撃やその他の種類の攻撃から公共サービスを提供する Web サーバーを保護
浄水場版・発電所版	産業用制御システムと重要インフラを保護

シナリオごとに過去の代表的なインシデントを元に作成されており、各業界においてサイバーセキュリティとインシデント対応手順の構築を効果的に行うためのリファレンスとすることができます。

サイバーセキュリティに関する意思決定能力を向上するための「サイバーセーフティ ゲーム」(ワークショップ)

この管理職向けの対話型ワークショップ(コンピューターとインストラクターの組み合わせ)は自身の業務におけるサイバーセキュリティの重要性についての動機付けを行い、自身の部門で安全な作業環境を維持するために重要な適性、知識、および意識を学ぶことができます。

組織は、サイバー脅威に対抗するためにIT セキュリティを準備し、コンプライアンスも含めたトレーニングを実施していることと思いますが、それだけでは十分ではありません。

- トレーニングによって従業員はサイバーセキュリティの重要性を理解して適切な行動をしているでしょうか?
- ビジネスの効率を低下させることなく、適切な強度のセキュリティを実現できているでしょうか?
- 日々のサイバーセキュリティ対策を実施するためのセキュリティ担当者の人数は十分で、現場の情報を効率よく収集し対処できているでしょうか?

これらの課題に対処するもっとも効率的な方法は、**管理職が自身と組織のビジネス効率を犠牲にせずサイバーセキュリティを実現する**ことです。日常的な従業員との対話やビジネスに関する意思決定を行うのは、**管理職の責務です**。日常的な意思決定においてサイバーセキュリティにも対処することが重要なのです。

Kaspersky サイバーセーフティゲーム(ワークショップ)は管理職が、自身の部門で安全な作業環境を維持するために重要な**適性、知識、および意識**の学習を効果的に支援します:

- 経営幹部や部門管理者が自組織に最適なサイバーセキュリティ対策を採用するための戦略の理解を促進
- サイバーセキュリティの観点をを強化することで、業務プロセスのサイバーリスクについての分析力を高める
- サイバーセキュリティに関する検討事項をビジネス戦略の重要事項として見なす
- 従業員に対して影響力を持つリーダーシップと有益な助言

KIPS は、カスペルスキーあるいはパートナーによってトレーニングを受講するだけでなく、自組織でトレーナーを育成して実施することが可能で、導入に際しての主な利点は次のとおりです:

- 実施が容易 – トレーナーはセキュリティの専門家でなくても構いません
- スケジュール調整が容易 – トレーニングはモジュール型で2時間単位で実施できますので、従業員のスケジュールに合わせることが可能

2017 年 2 月時点で 27 言語で利用可能です。

カスペルスキーのベストプラクティスガイドに従ってプラットフォームを使用することにより、測定可能で継続性のあるサイバーセキュリティ教育計画を立案して実装することができます。これにより、従業員のスキルレベルを効果的に高めることができ、脅威の状況と個人のスキルに応じてトレーニングを実施するセキュリティドメインを指定することができます。

デモについては、www.kaspersky.co.jp/enterprise-security/cybersecurity-awareness/demo/ を参照してください。

サイバーセーフティを実現するための従業員向けトレーニングプラットフォーム

重要になるのは基礎的なスキルと知識を全従業員が取得することです。よくあるシナリオや状況での判断に必要とされる、多大な知識を習得して潜在的な脅威とそれに対処する方法を理解するには、効果的かつ自発的な学習を促すことのできるトレーニングが必要です。カスペルスキーのオンライン対話型トレーニングプラットフォームは、効果的な学習環境を提供します。

オンラインの対話型トレーニングプラットフォーム

- 集中力を維持しながら短期間で完了
- 基礎となる知識とスキルを繰り返し強化
- 管理の自動化により管理者の負荷を低減
- 20 を超えるモジュールにより、すべてのセキュリティドメインに対応

知識の評価

- 定義済みまたはランダムな評価、顧客定義済みの質問、およびカスタマイズ可能な期間を提供
- すべてのセキュリティドメインに対応
- 膨大な質問ライブラリからランダムに問題を組み合わせた小テストによる知識の評価

模擬フィッシング攻撃

- 詳細に設定可能でリアルな、難易度が異なる 3 種別のフィッシング攻撃
- 従業員がフィッシングメールを開くたびに結果を記録して学習モジュールを表示
- 模擬攻撃の対処に失敗した従業員に対する追加のトレーニングモジュールの自動割り当て

レポート作成と分析

- 組織全体、部門別、拠点別、役職別、または個人レベルでの統計情報を提供
- 従業員のスキルレベルとその動向を監視
- 多数の形式またはお使いの LMS に対するデータエクスポートに対応

注目点

評価では、さまざまな観点からセキュリティに関する文化について注目します：

- 組織（経営）レベル
- 個人（従業員）レベル
- 使用可能な専門知識
- 1 つのプロセスとしてのセキュリティ保証

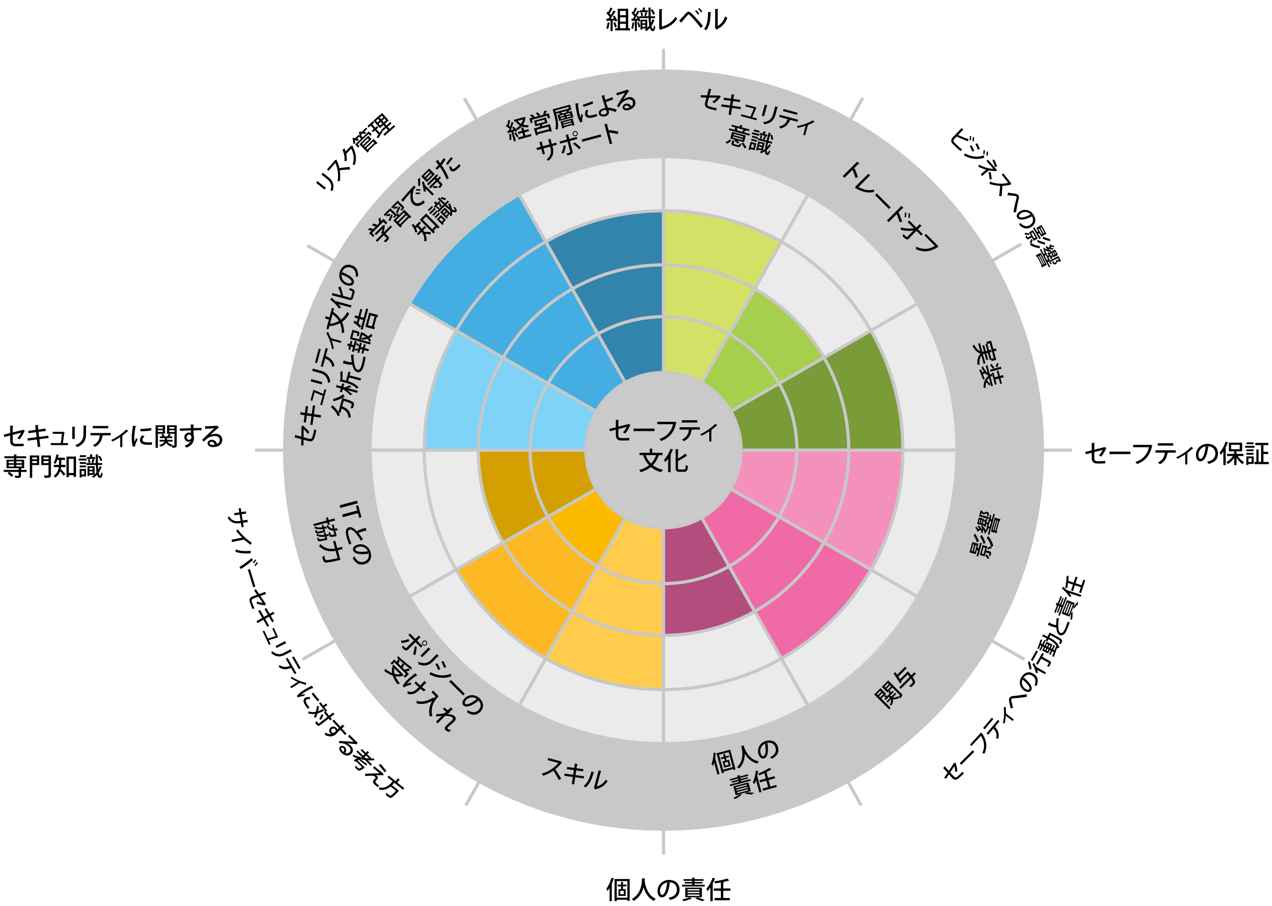
サイバーセーフティの習熟度を評価

サイバーセーフティに関する文化の評価では、企業のすべてのレベルで実際の日常的な行動と意識について分析し、組織の従業員がサイバーセキュリティのさまざまな側面についてどのように認識しているかを示します。

評価結果は、ドメインごとの理解のばらつきを確認し、さらに認識とトレーニング、社内での情報共有、ビジネスを進める上での原則を含む、セキュリティ部門の社内および社外アクティビティにおける優先事項の根拠付けと調整に使用できます。

サイバーセキュリティに関する文化は組織全体で評価して対策が講じるのが適切です。評価結果は、ビジネス効率をサポートする際のサイバーセキュリティの役割と位置付けに関する議論の基礎になります：

- サイバーセーフティ意識（セキュリティとポリシーに関する意識）
- リスク管理（ガイダンス、フィードバック、改良）
- 行動と責任（セキュリティに関する従業員の意識とふるまい）
- ビジネスへの影響（セキュリティとビジネス効率間の均衡）



サイバーセキュリティに関する文化を分析した報告書は、企業のセキュリティに関する技術的な成熟度レベルを評価しているものではなく、セキュリティ部門の効率の指標を示すものでもないことに注意してください。

この報告書は、一般従業員がサイバーセキュリティに関してどの程度意識しているのか、サイバーセキュリティに対する文化、習慣、日常的な行為や業務についてどのようなことを考えているのか、企業をサイバー脅威から保護する文化に関するさまざまな側面について個人的に意識しているのはどのようなことなのかを示すものです。このような意識は、単にセキュリティおよびリスク管理部門の努力の結果としてではなく、企業のさまざまな業務と社員の行動によって測るべきものなのです。

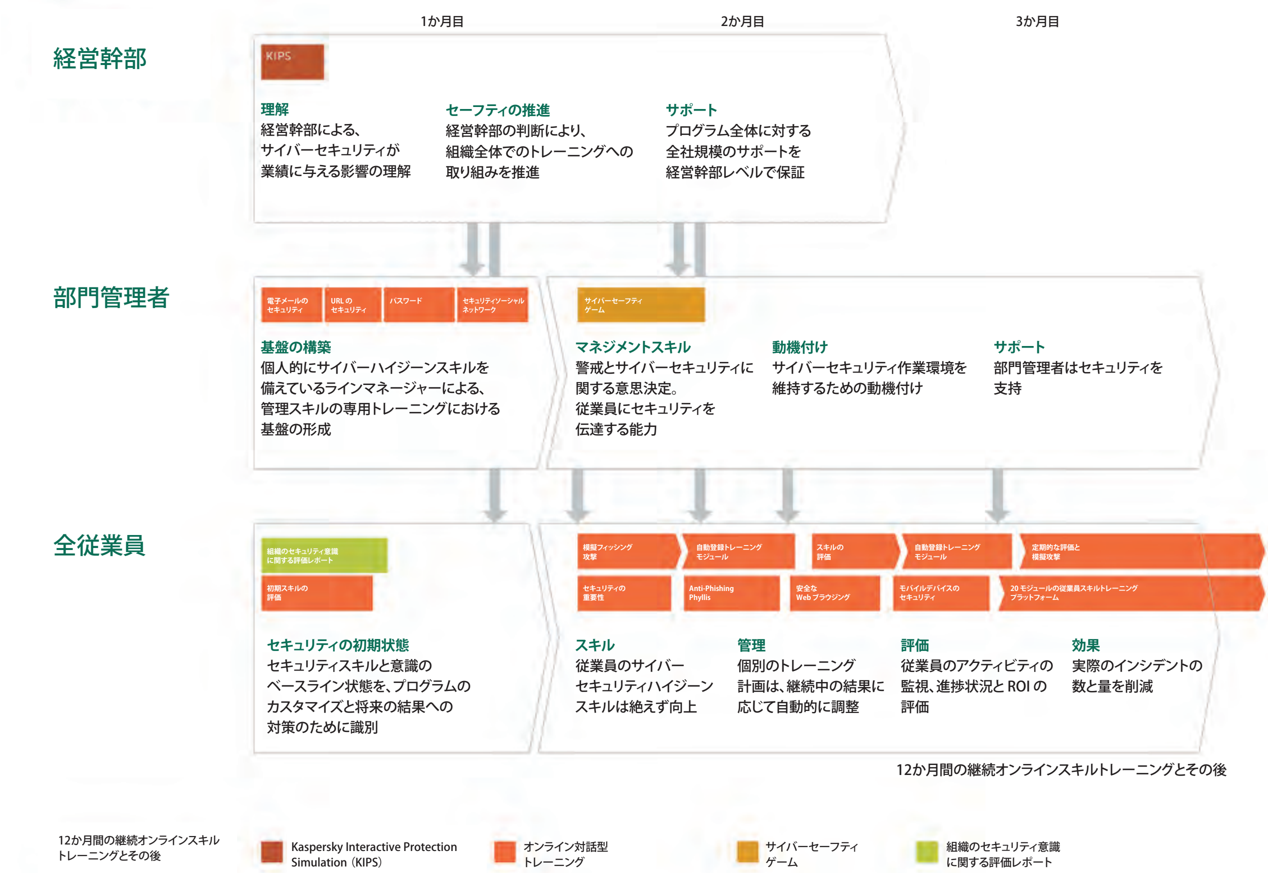
この評価は、クラウドを利用したの調査として実施されます。調査に要する時間は約 15 分で、すべての従業員に対して調査を実施するにはおよそ 2 週間を要します。

調査が完了した後、調査結果のレポートが提供されます。

組織全体でセーフティ意識を向上

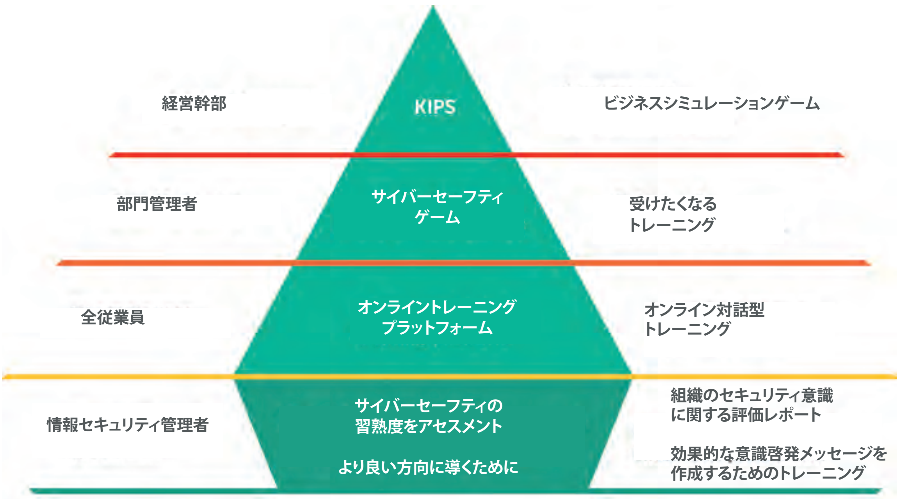
Kaspersky Security Awareness 製品を使用して従業員を教育する際の推奨導入手順です。当社では、お客様向けの具体的な手順と体系的なサポートをご用意しております。

組織全体のセーフティを向上 – トレーニング間でお互いをサポート



Kaspersky Security Awareness 意識啓発トレーニングプログラム

KIPS は、サイバーセーフティ意識啓発プログラム、Kaspersky Security Awareness の一部です。組織のすべてのレベルに対して、意識向上トレーニングとゲーミフィケーションを組み合わせたサイバーセキュリティ文化を醸成する作業を行う組織を支援します。



包括的でシンプル

- すべてのセキュリティドメインをカバー
- 親しみやすい環境
- 魅力的なトレーニング
- 効果的な演習
- 情報システムの専門家でなくとも理解が進む

ビジネス上の利点

相当する割合

93 %

従業員がサイバーセキュリティの知識を日常業務に活用する可能性

最大

90 %

インシデント数の減少割合

50 ～ 60 %

サイバーリスクによって失われる費用を削減

増大した割合

30 倍以上

セキュリティ意識啓発への投資の ROI

www.kaspersky.co.jp

KLSA20170915

株式会社カスペルスキー
Enterprise Cybersecurity：www.kaspersky.co.jp/enterprise-security/
Kaspersky Security Awareness：www.kaspersky.co.jp/enterprise-security/cybersecurity-awareness
製品デモ：www.kaspersky.co.jp/enterprise-security/cybersecurity-awareness/demo/