KnowBe4
Human error. Conquered.

セキュリティカルチャー構築・強化ガイド

The Security Culture How-to Guide

セキュリティカルチャーの構築と強化に向けて取り組むときの7つの基本ステップ

セキュリティカルチャー構築・強化ガイド

内容

はじめに

「セキュリティカルチャー（文化）」という言葉は、ここにきて、広く使用されるようになってきています。その中、セキュリティカルチャーは、セキュリティ担当者との会話や組織内でのテーマとして話題に上るようになってきています。また、メディアでも、セキュリティカルチャーをテーマに取り上げることが増えています。しかし、この言葉の意味合いは、人によって異なり、明確な定義がありません。また、組織内で優れたセキュリティカルチャーの構築への取り組みを始めようとする場合に、どのようなステップを踏むべきかは、さらに不明瞭になっています。多くの組織は、セキュリティカルチャーとは何か、そして優れたカルチャーを実現するために何をすべきかについて、漠然としたイメージしか持っていないと言えるのではないでしょうか。

本ガイドでは、セキュリティカルチャーの基本概念を定義し、組織内で優れたセキュリティカルチャーの構築を醸成するためにどのような行動指針を検討すべきかを解説していきます。セキュリティカルチャー（文化）には、様々な側面があります。本ガイドは、セキュリティカルチャーの個々の側面について深掘りすることを目的にしていません。読者の皆様が、セキュリティカルチャーの基本事項や、組織のセキュリティカルチャーを適切な方向へと舵取りするために必要なステップを理解できるようにすることを目的にしています。今後、セキュリティカルチャーの各要素について詳解するガイドを提供する予定です。

最初に、一朝一夕では、優れたセキュリティカルチャー（文化）を築けないことを理解してください。真摯な努力を続けることが、大きな成果につながります。セキュリティカルチャー（文化）を組織に刷り込み、文化として確立できれば、維持することが容易になります。この良い例が、新入社員の入社時にセキュリティカルチャー（文化）を刷り込むことで早期に順応させることができることです。

私たちは社会的な生き物であり、「習うより慣れろ」という諺が当てはまる振る舞いは多くあります。新しい仕事を始めるときには、目にする他者の多くの行動を無意識のうちに取り入れるようになります。例えば、ワークステーションから離れるときに必ずロックするカルチャーが組織に根付いていれば、新入社員は「この会社ではこうするものだ」と普段から感じることができ、意識することなくこのような習慣を身に付けることができます。これが、強固なセキュリティカルチャー（文化）が根付いている環境がもたらす利点です。このような成熟した文化が醸成されていれば、全社的に維持することが容易になります。

セキュリティカルチャーの定義

多くの組織にとって、セキュリティカルチャーを定義することは、決して容易ではありません。セキュリティカルチャーとは何かをしっかりと理解し、組織のセキュリティカルチャーの方向性を十分に検討することがなければ、効果的で持続的な変化を組織にもたらすことはできないでしょう。KnowBe4では、セキュリティカルチャーを「組織のセキュリティに影響を与える組織共通の考え方、習慣、社会的な振る舞い」と定義しています。

このように定義しておくと、セキュリティカルチャーをより簡明に捉えることができます。セキュリティの観点だけではない広義での「カルチャー（文化）」には、「他人が見ていないところで、共有の考え方や価値基準のもとに無意識に何をするのか」という側面があります。これは、人間の「誠実さ」や「性格」という言葉に例えられることも多くありますが、組織として見る場合には「カルチャー（文化）」と表現できます。

組織のセキュリティカルチャーの変革に取り組むときには、この定義を基本理念として周知徹底することは極めて重要です。プリントアウトして、目につくところにメモを貼っておいてもいいでしょう。これにより、目標を常に意識して、取り組みを継続できます。

セキュリティカルチャーの7つのディメンジョン（基軸）

KnowBe4のリサーチ部門が2019年に公開したホワイトペーパー「セキュリティカルチャーの7つのディメンジョン（基軸）」では、セキュリティカルチャーの7つのディメンジョンを定め、これらのディメンジョンを使用して組織のセキュリティカルチャーを評価する方法を解説しました。7つのディメンジョンは、以下の通りです。

- **セキュリティやポリシーに対する社員の姿勢/態勢（Attitudes）**
- **振る舞い・習慣的行動（Behaviors）**
- **セキュリティに関する問題や活動に対する認知（Cognition）**
- **セキュリティに関連する報告・連絡、コミュニケーション（Communication）**
- **セキュリティポリシーのコンプライアンス（Compliance）**
- **組織の暗黙のツール、常態・常識（Norms）**
- **個人の責任感（Responsibility）**

これらのディメンジョンの詳細や、セキュリティカルチャーの評価に使用する方法については、詳細な資料を読むことをお勧めします。現時点では、これらの7つのディメンジョンがあることを意識しておくだけで十分です。これについては、組織のセキュリティカルチャーの改善に着手するときには、1つまたは2つのディメンジョンにまたがる習慣的な行動や振る舞いを選んで集中的に取り組むことを推奨します。それ以上多くのディメンジョンにまたがる行動や振る舞いを選ぶと、1つまたは2つに焦点を絞って取り組む場合と比較して、行動変容が現れるまでに長い期間を要することになります。また、ここで注意しなければならないことは、各ディメンジョンは単独では存在しているのではないことです。あるディメンジョンの習慣的な行動や振る舞いを改善することで、往々にして、他のディメンジョンでの行動変容が引き起されます。

セキュリティカルチャー醸成への段階的進化のABC

セキュリティカルチャーをいかに変革するかを考えるときの重要な概念が「ABCの基本理念」です。このABCは、以下の単語の頭文字を取った略称です。

- Awareness（意識変革）
- Behavior（行動変容）
- Culture（カルチャー醸成）

意識向上（Awareness）は、Behavior（行動）に影響を与え、行動変容を起こし、Culture（カルチャー醸成）につながる。この段階的な進化は、セキュリティカルチャー醸成の基本理念の要となる。

これはシンプルでありながら重要な基本理念です。意識向上（Awareness）は、Behavior（行動）に影響を与え、行動変容を起こし、Culture（カルチャー醸成）につながります。この段階的な進化は、セキュリティカルチャー醸成の基本理念の要となります。意識向上から意識変革が起り、自動的に行動変容が生まれてくるわけではありません。ここでポイントとなることが、セキュリティを強化することが重要であることを共感してもらうことです。この共感の輪が、大きな影響となって派生してくることです。

ここでももう1つのポイントが、一人の行動が変わっても、組織全体の行動変容とならないことです。ここでも同様に、行動変容の輪が拡がり、組織全体の行動変容へと拡大し、組織全体の行動が変ることで、組織のカルチャーに変化が生まれてくるのです。

さあ始めよう！

ここまでは、セキュリティカルチャーに関する基本的な考え方や定義について説明してきました。ここからは、セキュリティカルチャーをいかに変化させるかについて説明します。この取り組みを始めることは、決して容易ではありません。では、この取り組みに着手するには、何をしたらよいのでしょうか。専任のセキュリティカルチャー担当者を任命して、人の行動を変える行動科学について正式なトレーニングを受けさせれば良いのでしょうか。このようなアプローチは、総論ありきで、なかなか結果を生み出すものではありません。KnowBe4はこれまでセキュリティカルチャーに対して多大な投資をしてきています。KnowBe4は、セキュリティ意識、セキュリティ行動習慣性、セキュリティカルチャーに関する膨大なデータセットを有しています。

長年にわたり培ってきたデータドリブンの知見から生まれた、セキュリティカルチャーの改善を継続するサイクルを作り出す基本的な7つのステップを以下に紹介します。以下のページで、各ステップについて詳しく説明します。

ステップ1 - 変える必要がある従業員の危険な行動を1つか2つに絞って選択する

ステップ2 - 小さな行動変容を全社的に波及させる計画を立てる

ステップ3 - 経営幹部の賛同を得る

ステップ4 - 周知徹底のためのコミュニケーション

ステップ5 - 計画を実行する

ステップ6 - 結果を測定する

ステップ7 - さらに前進させる戦略を立てる

ステップ1 - 変える必要がある従業員の危険な行動を1つか2つに絞って選択する

ここで重要なことは、皆さんの組織が直面しているリスクをまずは理解することです。次に、集中的に取り組むべきディメンジョン（基軸）と危険な行動を特定することです。この絞り込みプロセスによって、取り組むべき対象が曖昧になることを避けることができます。ここでのポイントは、皆さんの組織が抱えている最も大きなリスクに合わせて、改善すべき危険 な行動に絞り込むことです。リスクは、多くの場合、「Risk（リスク）= Likelihood（発生する確率） × Impact（発生する影響度）」の式を使って数値化することができます。

ここで注意すべきことは、皆さんの組織が取り組むべきリスクや改善すべき行動は、一般的なリスクや行動ではなく、皆さんの組織に最も影響を及ぼすものにすべきことです。また、この絞り込みプロセスは皆さん組織の脅威モデルやリスクへの対応力も影響します。Verizonデータ侵害調査報告（Verizon 2022 Data Breach Investigations Report）などの最新の年次レポートを参照することで、取り組むべき現行の重大な脅威に関する知見が得られる場合もあります。

一度に多くを変えようとせず、十分な時間をかけて徐々にセキュリティカルチャーを変えていくことを目指しましょう。

例えば、電子送金詐欺は大きな脅威になっているか？ランサムウェアは自社にとって深刻なリスクか？物理的な脅威は重大な問題か？このような最新情報を把握することで、セキュリティカルチャーを改善するプログラムの方向性が明確になる場合があります。このような最新情報を把握することで、セキュリティカルチャーを改善するプログラムの方向性が明確になる場合があります。

一度に多くを変えようとせず、十分な時間をかけて徐々にセキュリティカルチャーを変えていくことを目指しましょう。最初に、1つか2つのディメンジョンにまたがっている危険な行動を選択し、3ヶ月から6ヶ月の期間をかけて変化させていきましょう。最初に1～2回のこのようなプロセスを経験してから、どのような変化が組織にもたらされるのかを確認し、取り組みを今後進めるペースを調整してもよいでしょう。大切なのは、特に初期段階で積極的になりすぎて、あまりにも多くのことを迅速に変えようとしないことです。

セキュリティカルチャーに関する調査を実施すると、最も改善が必要なディメンジョンを特定することができ、どのような危険な行動を中心に改善すべきかが明確になる場合があります。あるディメンジョンを改善することで、他のディメンジョンにその効果が波及することがあります。例えば、従業員がセキュリティポリシーを無視するなど、セキュリティに対する関心度が低い場合があります。この場合は、重要な内部規定が遵守されず、ランサムウェアに感染するリスクも高まります。ポリシーが自分の情報の安全性にどのような影響を与えるかを教育し、ポリシーに対する意識を向上させることに集中的に取り組めば、従業員によるポリシーの遵守状況を改善できる可能性があります。この場合、1つのディメンジョンに集中して取り組んだ成果して、2つのディメンジョンに良い影響がもたらされ、ランサムウェアに感染するリスクを低減できます。これは、ディメンジョンが相互に作用していることを示す一例です。

ステップ3では経営幹部の賛同を得るようにしますが、ステップ1のタイミングでも直属の上司にはセキュリティカルチャーの向上に取り組むことの重要性を伝える良い機会になります。この詳細については後述しますが、このような取り組みを進めていることを上司に意識してもらうだけで、上司からサポートを得ているように感じることができ、後でリソースが必要になったときに役立つ下地を作る機会にもなります。

ステップ2 - 小さな行動変容を全社的に波及させる計画を立てる

ポリシーを作成または変更する場合のように、正式なプロセスを踏んで、危険な行動を改善することができますが、経営幹部が模範となる行動をトップダウンで示すことで、行動変容を引き起こすことができます。

例えば、喫煙のためにオフィスビルの裏口を開放していた場合、このような喫煙休憩は認められないことを明記した社内規定を作成あるいは更新して従業員に正式に通告できます。しかし、喫煙していた経営幹部がこの裏口を率先して閉めて、ドアが開放されていることのリスクを伝えることで、トップダウンで指示することができます。正式に社内規定の変更を通告しなくても、他の従業員がその習慣を理解して、この小さな行動変化を全社に波及させることができます。それぞれの方法に利点と欠点がありますが、どちらも従業員の危険な行動を変えることができます。

他の人と一緒に働くことによって気付きが得られる場合、より早く、より少ない労力で行動変容を実現できるようになります。

人の行動を変えることは、最初は難しく感じるかもしれません。特に、技術的な変更が伴う場合は、尚更そのように感じられるでしょう。新しいテクノロジーを全社展開することを考えると、部門別に展開して、全社展開に実現することができます。全社展開を進めるときの依存関係を考慮し、不足している要素がある場合、準備するために時間がかかることを理解してください。想定される失敗を考え、リスクを軽減する方法を考えることも大切です。部門別の展開事例を適用して、全社展開していくことができるでしょう。

計画を立てるときには、自分の部署に所属しない人物であっても、セキュリティカルチャーの改善に影響を与えることができる人物を必ず見つけるようにしてください。組織の中には、少なくとも何人かは元々セキュリティに対して意識の高い従業員がいるものです。このような人物はインフルエンサーとして大きな力をもっており、模範となる振る舞いを示し、提唱することで、計画を大規模に実行するときに絶大な影響力を発揮します。このような人物を計画に組み入れるようにしましょう。他の人と一緒に働くことによって気付きが得られる場合、より早く、より少ない労力で変化を実現できるようになります。

本来、人は社会的な存在であり、自分では気が付いていなくても、他者の行動に同調し、同化する傾向があります。このような人物を特定して協力してもらうことで、重要なメッセージを発信するチャンピオンが組織のあらゆる場所にいるような効果を期待できます。また、グローバル企業であれば、これらの人物は、文化の違いを考慮しながらメッセージを発信してくれるでしょう。これらのセキュリティ意識が高い人物は、セキュリティカルチャーを改善するプロジェクトを全社的に成功させる重要な鍵を握っています。このプロジェクトを担当するあなたやあなたのチームは、組織のすべての部門

で簡単に活動できるわけではありません。そのため、企業のあらゆる場所におり、プロジェクトを支援してくれるセキュリティ意識の高い人物のサポートが必要となります。

ステップ3 - 経営幹部の賛同を得る

計画を作成したら、経営幹部の賛同を得る必要があります。経営幹部向けの事業計画の概要を準備しましょう。この計画書では詳細について触れる必要はなく、セキュリティカルチャーを改善することが必要な理由、変えない場合の組織へのリスク、計画に関与する人物、必要なリソース、予定されるタイムラインなどに重点を置いて作成してください。

経営幹部自らがセキュリティに関連する危険な行動を変えるように約束してもらい、行動変容に取り組んでいることを組織の他の部門に伝えてもらいましょう。

この時点で詳細な情報を求める経営幹部はほとんどいないはずです。経営幹部が意思決定するために必要なレベルの情報を提供できるように準備しておきましょう。可能であれば、経営幹部自らがセキュリティに関連する危険な行動を変えるように約束してもらい、行動変容に取り組んでいることを組織の他の部門に伝えてもらいましょう。
小さな変化を積み上げていく手法は、非常に有効です。例えば、経営幹部に対して、離席するときは必ずPCをロックするように求めます。これは簡単な取り組みですが、模範となる行動を行っていることを他の従業員に伝えることにつながります。

特に、大きな摩擦を生じさせることなく、振る舞いを改善する取り組みを効果的に進めることができることを証明できれば、このような改善サイクルを何度か繰り返し、振る舞いを改善させていくことがさらに容易になります。

経営幹部とこの課題について話すときは、以下のような端的な説明でアプローチしても良いでしょう。

> *「私たちの業界では、ランサムウェアが最も大きな脅威になっています。ランサムウェア攻撃を受けて支払う身代金の平均額は57万ドルに達しており、被害を復旧するためにかかる費用はこれよりもはるかに高額です。フィッシングメールはランサムウェアに感染する最大の原因です。ランサムウェアに対する防御を強化するために、フィッシングメールを特定しセキュリティチームに報告する能力を従業員が向上できるように取り組んでもらいたいと考えています。従業員全員が参加する今後の会議で、この取り組みについて言及していただけないでしょうか。詳細については後でご連絡いたします。ご支援どうぞよろしくお願いいたします。」*

これは、要件をシンプルに伝えており、詳細には触れておらず、エレベーターピッチとして十分な短さです。経営幹部に無理な確約を求めるのではなく、この取り組みを支援してもらうように依頼します。もちろん、組織の特性や経営幹部の性格に合わせて、別の方法でコミュニケーションしなければならない場合もあるでしょう。また、数名のマネージャーや経営幹部、特にレポート先となる上司に支援を約束してもらう必要があるかもしれません。先のストーリーは、1つのアプローチとして参照してください。従業員は、経営幹部が模範となる行動や態度を示してくれることを期待しています。また、優れたセキュリティカルチャーを醸成するためには全社員が責任感を持つ必要があることを理解してもらうために、経営幹部がこれらの活動を受け入れていることを伝える方法を検討してください。

ステップ4 - 周知徹底のためのコミュニケーション

ステップ4では、行動を改善する「理由」を従業員に伝えます。振る舞いを改善する理由を説明して理解してもらうことは、非常に重要なプロセスです。なぜなら、セキュリティカルチャーを向上させるためには、同じ操作を完了する場合に、追加の作業を求めることが多いためです。

例えば、数分でも離席するとパソコンがロックされるケースを考えてみましょう。特に何も操作しなくてもコンピューターをロックするように簡単に設定できますが、席に戻ってきたときにはロックを解除しなければなりません。離席して休憩室でコーヒーを飲むだけでも、離席するときにはコンピューターをロックし、戻ってきたときにはパスワードを入力してロックを解除するように依頼することになります。そのため、勤務時間中にパスワードを入力する回数はかなり増加します。もしも、行動を改善する理由を理解してもらえずに、自分には関係ないと思われると、摩擦が生じる恐れもあります。

行動を変えてもらい、セキュリティカルチャーを改善させるために、コミュニケーションは重要な役割を果たします。このようなメッセージをメールで従業員に発信し、セキュリティカルチャーを改善する取り組みを実施していくことを知らせると役立つ場合があります。さらに効果的なのは、経営幹部にこのようなメッセージを発信してもらうことです。

> *清掃員や保守担当者、あるいは求職者を装うソーシャルエンジニアリングの手法で、オフィスビルに侵入し、ウイルスをインストールするためにロックされていないコンピューターを探し回るサイバー犯罪者が増加しています。コンピューターがロックされていなければ、一瞬でウイルスが仕込まれてしまいます。ウイルスに感染すると、従業員のデータや個人情報が窃取される場合もあります。*
>
> *このような問題を避けるため、また、自分自身あるいは同僚の安全を守るために、コンピューターから離れるときは(たとえ1分であっても)、必ずロックするというポリシーを実施することになりました。従業員全員の安全を確保するためのご協力をお願いします。*

セキュリティカルチャーを改善させるために重要なのは、この取り組みを進めるときの従業員との摩擦を取り除くことです。このためには、コミュニケーションのトーンも重要になります。

これは伝え方の一例です。行動を改善することがどのように個人に関係するのかを示しながら、変更内容について伝えるようにしています。場合によっては、正式で直接的なコミュニケーションが効果的となる場合もあります。セキュリティカルチャーを改善させるために重要なのは、この取り組みを進めるときの従業員との摩擦を取り除くことです。このためには、コミュニケーションのトーンも重要になります。従業員がセキュリティチームを、敵対する勢力はなく、自分にとって有益な味方のように感じてくれるようになれば、通常、より優れた成果を得ることができます。

ステップ2では、この取り組みを理解して支援してくれるチャンピオンについて説明しましたが、このコミュニケーションの段階は、チャンピオンに関与してもらう最適な機会です。彼らは、訴求力のあるメッセージを、わかりやすく、関連を持たせて伝えることができます。また、本社の見知らぬ誰かに、頭ごなしに「これをしてください」と言われるのではなく、同僚や知っている人物に「安全のためにこれをしたほうがいいよ」と言われるほうが、高い効果を期待できます。このときに重要となるのが、強い影響を与え、重要なメッセージを発信する能力です。

さらに、組織の他の部署とも連携し、コミュニケーションの方法を考えてメッセージの訴求力を強化してください。例えば、マーケティングチームと連携すれば、コミュニケーションの方法に関するヒントや手法についてインプットしてもらうことができます。また、ITチームに依頼して、会社のイントラネットサイトにバナー広告を掲載してもらうこともできるでしょう。人はさまざまな方法で情報を認識しますので、目に触れる機会が多いほど、メッセージを理解してもらいやすくなります。

ステップ5 - 計画を実行する

計画を立案するときには、成功のあるべき姿を明確にし、目標を立てなければなりません。計画の各部についてコミュニケーションして実行するための期限と期間について、ここまでの段階ですでに練られているはずです。計画には多少の柔軟性を持たせなければなりませんが、期待される成果を常に意識し、可能であれば途中段階で効果を測定しましょう。

計画を実行する前に、セキュリティカルチャーに関する調査を実施し、組織の現状を測定しておくとよいでしょう。この調査では、7つのディメンジョンについて自社の状況を把握することができ、どれだけ改善されたかを比較するベースラインを得ることができます。

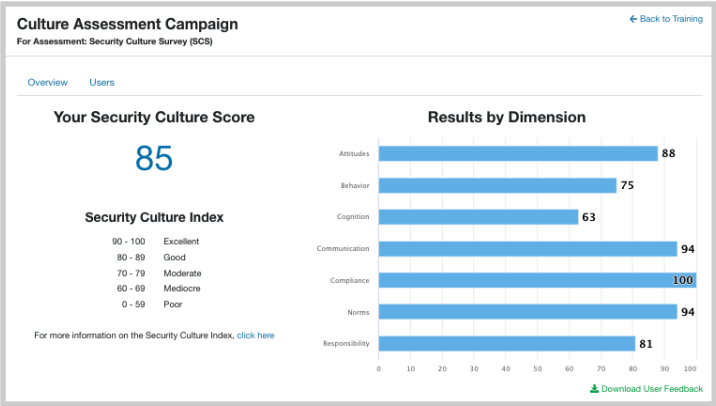
また、取り組みへの賛同者を全社的に特定して、必ず協力してもらいましょう。また、彼らが支援できる方法や質問への回答を得るためにどうすれば良いかについても、必ずコミュニケーションをとってください。

習慣を変えることは容易ではありません。何かを変えようとすると、反発する人は必ず存在します。ただし、反発を個人への攻撃として受け止めないでください。可能な限り、解決できるように努力してください。また、これらの計画の一部が実際に生産性に悪影響を及ぼすことが判明する場合もあります。そのような問題について常に留意し、問題があれば調整し、次のサイクルを計画するときに対応を考えてください。

また、計画を推進し、成功を促進させるために、コミュニケーションを活用することも重要です。うまくいっているプロジェクトや、前向きな変化に取り組んでいる人物にスポットを当てる方法を考えてください。

ステップ6 - 結果を測定する

計画を完全に実行したら、再度「セキュリティカルチャーに関する調査」を実施し、効果があった領域と、さらに改善が必要な領域を明らかにできます。調査で得られた情報をもとに、組織にとってより効果的なアプローチを見つけ、改善しながら実行していくことが可能になります。あるディメンジョンにおける振る舞いの改善が、他のディメンジョンにどのような影響を与えるかを把握することで、自社におけるディメンジョン間の関係を深く理解し、今後の計画をさらに改善できるようになります。



この結果は報告書にまとめ、リーダーと共有しましょう。この結果には、詳細な情報を記載する必要はありませんが、結果をまとめて報告することで、計画を改善し、経営幹部や上司からの継続的な支援を取り付けることが非常に容易になります。報告書には、計画を実施する前後の結果や、結果として得られた目に見える変化も必ず記載しましょう。例えば、以下のような情報を記載してください。

「<チーム名を挿入>が直近で完了したセキュリティカルチャーの改善計画の結果を報告します。

従業員のセキュリティポリシーに対する態度が20%改善され、ポリシーを遵守する従業員の割合は15%向上しました。また、ウイルスの削除を要求するヘルプデスクへのチケット数は20%減少し、フィッシングメールの報告も32%増加しました。これにより、サイバー攻撃の標的となっている領域を明確に把握できるようになり、さらに優れた防御が可能になります。セキュリティカルチャーを改善する取り組みを今後も継続したいと考えています。今後、本件についてディスカッションする機会を設けていただくようにお願いいたします。

繰り返しになりますが、これはコミュニケーションの一例にすぎません。結果を伝える方法は、報告する組織や経営幹部によって異なります。

また、データの見せ方にも配慮してください。また、部門別や経営幹部別に結果を提供することで、組織で厳格に運用する必要がある領域が浮き彫りになり、緊急に対応しなければならないことがわかる場合もあります。誰しも上司にはいいところを見せたいものです。特定の部門や幹部の結果が特に悪い場合、脆弱になっていることの矢面に立たされることがないように配慮することも大切です。

ステップ7 - さらに前進させる戦略を立てる

タイムラインに沿って計画を完了した後、または計画した目標を達成した後には、自社の脅威を見直し、今後実施するサイクルで同じ目標に引き続き焦点を当てるべきか、他の目標を設定して取り組むべきかを判断できます。

うまくいったことと、うまくいかなかったことを振り返り、今後の目標を調整することで、次回実施するときに成功する確率を高めることができます。プロジェクトを一度完了したら、賛同者（インフルエンサーやチャンピオン）として協力してもらった方々に連絡を取り、フィードバックや今後改善に取り組むべき行動について提案してもらう良いタイミングとなります。このときに、自分の部署では聞けないような貴重な情報を得られる場合もあります。

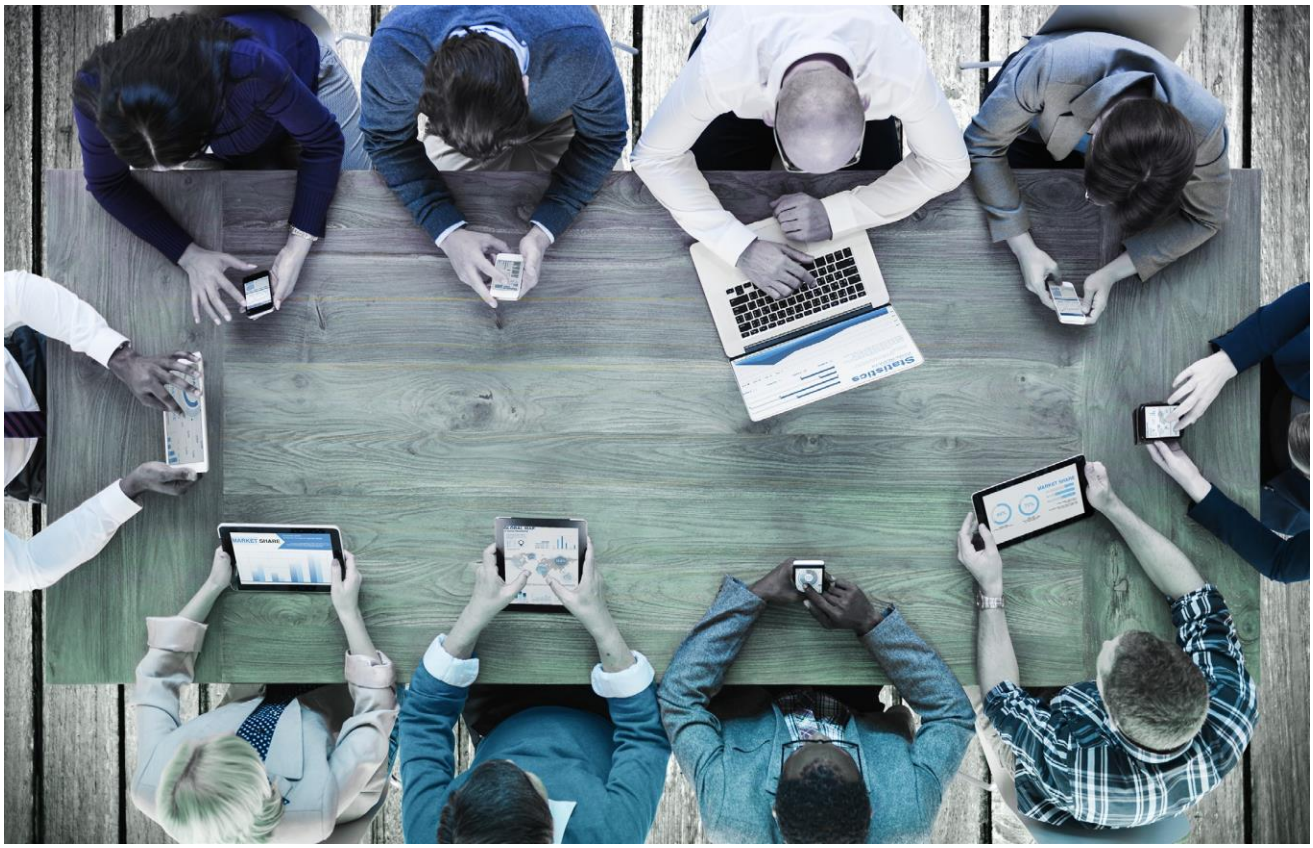
今後改善する行動を変更することを決めたら、これまで取り組んできた行動が、元に戻ることがないように、改善を継続してください。一つの行動を改善しても大きな効果を得ることはありません。継続的に調整しながらいくつかの行動を改善することで、組織全体のセキュリティカルチャーを前進させることが可能になります。

まとめ

セキュリティカルチャーを改善することは、特に最初のうちは複雑に感じられるかもしれません。しかし、時間をかけることで着実に改善させることができ、正しい方向に導き、習慣を形成できることを理解すれば、タスクを簡略化できます。計画的に行動し、あまり性急に変化を求めないことです。コミュニケーションによって、セキュリティを改善しなければならない理由を理解してもらうことができれば、行動を改善する速度と度合いに大きな違いが生まれます。

本書では主にオフィス環境におけるセキュリティカルチャーの改善計画について説明してきましたが、セキュリティ意識の向上とカルチャーの醸成について学んだことはすべて自宅の環境にも同じように適用できます。友人や家族などの大切な方々のセキュリティを高めるために、本書で習得した内容を活かしてください。

今後、本書で簡単に取り上げた7つのディメンジョンをさらに掘り下げ、セキュリティカルチャーが改善されるにつれて役立つ専門的な情報を提供する予定ですが、改善計画に取り組むときには、本書と以下のチェックリストを活用してお役立てください。取り組みを早く始めるほど、成果を早く得ることができます。



セキュリティカルチャー改善計画のチェックリスト

ステップ1：変える必要がある従業員の危険な行動を1つか2つに絞って選択する

- ☐ リスクに応じて改善すべき危険な行動を1つまたは2つに絞って選択する
- ☐ セキュリティカルチャーに関する調査を実施し基準値を設定する

ステップ2：小さな行動変容を全社的に波及させる計画を立てる

- ☐ セキュリティカルチャーの改善計画を実施するタイミングと期間を計算する。
- ☐ 組織に存在するアンバサダー（インフルエンサー）／チャンピオンを見つける。

ステップ3：経営幹部の賛同を得る

- ☐ 経営幹部が確認でき、支援を約束してくれるような計画の概要書を作成する。
- ☐ これらの取り組みに対する経営幹部の支援を取り付ける。

ステップ4：周知徹底のためのコミュニケーション

- ☐ セキュリティカルチャーが自分に関連することを理解してもらうことに重点を置いた従業員向けのコミュニケーション計画を作成し、他部門と提携しながらメッセージが浸透するように努力する。
- ☐ サポートが必要な従業員がいればサポートし、懸念を持っている従業員には懸念を払拭できるように努める。

ステップ5：計画を実行する

- ☐ 具体的な成功のイメージとタイムラインを明確にしてゴールを設定する。
- ☐ 賛同者であるセキュリティチャンピオンや経営幹部とコミュニケーションを図り、サポートを提供する。

ステップ6：結果を測定する

- ☐ セキュリティカルチャーに関する調査を再実施して前回の結果と比較する。
- ☐ 調査結果の概要を記した経営幹部向けの報告書を作成する。

ステップ7：さらに前進させる戦略を立て、そのサイクルを繰り返す

- ☐ 賛同者からフィードバックを得るとともに、次回実施するサイクルを向上するためのアイデアを得る。
- ☐ 脅威を検証し、次のサイクルの行動目標を決定する。

その他の関連情報

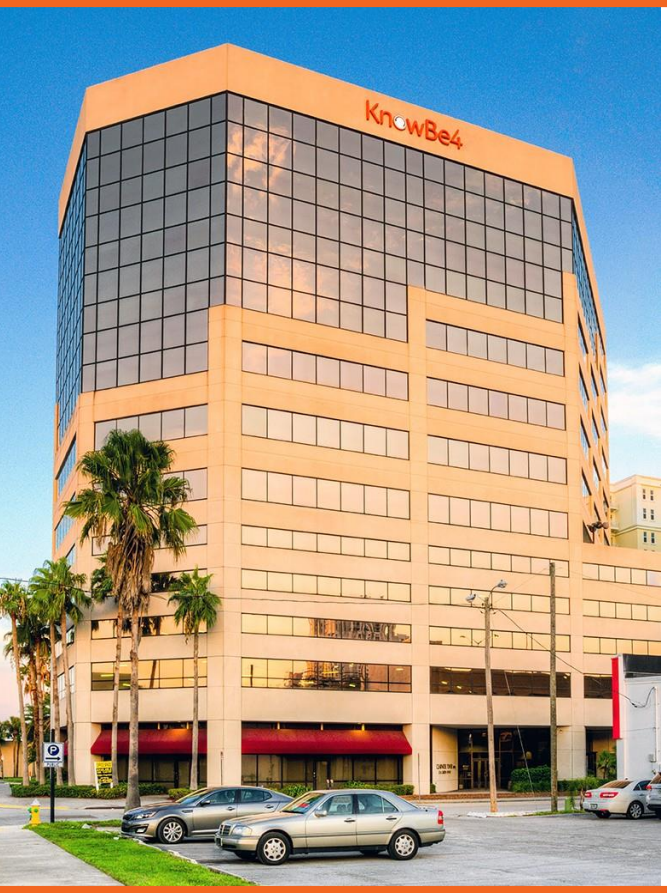
フィッシングセキュリティテスト
あなたの企業や組織の従業員の何パーセントがフィッシング攻撃に引っかかるかをスコア化することができます。

セキュリティプログラムビルダー
あなたの企業や組織のためにカスタマイズされたセキュリティ意識向上プログラムの作成を自動化します。

Phish Alertボタン
あなたの企業や組織の従業員がフィッシング攻撃の報告をワンクリックで行うことができます。

無償Email Exposure Checkツール
あなたの企業や組織の従業員のメールアドレスが、どれくらいインターネット上で公開されているかをチェックできます。

無償なりすましドメインテスト
ハッカーがあなたの企業や組織のドメインのメールアドレスを偽装できるかをチェックできます。



KnowBe4は、セキュリティ意識向上トレーニングとフィッシングシミュレーション・分析を組み合わせた世界最大の統合型プラットフォームです。セキュリティの人的要素への抜本的な対策の欠如に気づき、KnowBe4は「人」を狙うセキュリティ脅威から個人、組織、団体を防御することを支援するため設立されました。

KnowBe4プログラムは、偽装攻撃によるベースラインテスティング、クラウドベースのインタラクティブなトレーニング、継続的なアセスメントを組み合わせた統合型のアプローチです。ここには、フィッシング、スミッシングといった多彩な偽装攻撃を通しての本番さながらのフィッシング体験とトレーニングがあります。セキュリティ第一のマインドセットを形成し、組織全体のセキュリティカルチャーを醸成します。

2022年12月現在、5万6千社を超える企業や団体がKnowBe4を採用して、防御の最終ラインとして「人」による防御壁を構築しています。

詳しくは、**www.KnowBe4.jp**をアクセスしてください。

KnowBe4
Human error. Conquered.

KnowBe4 Japan 合同会社　〒100-6510 東京都千代田区丸の内1−5−1
新丸の内ビルディング10F　EGG 内
Tel: 03-4586-4540 | www.KnowBe4.jp |