iSiD

KnowBe4
Human error. Conquered.

セキュリティ「文化」を考える

2021

著者

アルテア・セキュリティ・コンサルティング
代表
二木真明

思考停止にならないセキュリティを目指して

本ホワイトペーパーは、セキュリティ有識者である著者が客観的な視点で記載したドキュメントです

OptimizingYourSecurity

内容

初版　2020年6月1日
更新　2021年6月1日

はじめに

生活やビジネスの大部分を ICT に依存している「サイバー」時代、コンピュータやネットワークの能力は劇的な向上を続けています。新たな技術が次々と登場し、「人工知能」とも呼ばれる深層学習の応用により、従来、人が担ってきた領域までも、機械化、自動化が進みつつあります。しかし、それらが人の手による産物であり、人による社会やビジネス、生活を補助するための道具として作り出されたものである限り、依然として人は、それらの使い手であり続けます。様々な考え方を持つ人がいるように、これらの道具の使われ方も様々です。機能や能力が向上すればするほど、誤った目的や悪意を持った使い方がもたらす結果は深刻なものとなります。つまり、サイバー技術が進化すればするほど、人はより慎重に、高い倫理観を持って、これらを使わねばならないのです。

近年頻発している「サイバー攻撃」や「サイバー犯罪」は、悪意を持った使われ方の典型的なものでしょう。一方、これらの被害を受ける側にも「油断」があります。少し慎重に対処していれば、避けられた被害も少なくありません。技術的な対策も可能ですが、そればかりを強化すれば使い手の自由度を低下させ、生産性や創造性を損なう危険があります。ICT の使い手には、その自由度に応じて、こうした脅威の存在やその目的、手段を意識して、つけいる隙を与えないことが求められますが、これは一般に簡単ではありません。

本書では、企業・組織の ICT 利用における「人」に着目して、こうしたリスクを下げる方法を考えます。

1. すべてがICTに依存する現代

想像してみてください。世の中にコンピュータやネットワークがなかったら、家庭での生活や職場での仕事はどのようになるでしょう。パソコンやネットワーク、様々なサーバが使えなかったら、デスクワークはすべて紙と鉛筆と消しゴムの世界に戻ってしまいます。生産現場ではロボットや自動化された加工装置などの一切が使えず、昔ながらの手作業に戻ります。家庭においても、いわゆる「デジタル家電」はすべて使えなくなり、昔ながらのアナログな世界に戻ります。今から50年ほど前の世界を想像すればいいでしょう。この時代を知っている人たちは、それでも生活や仕事に問題はなかったと思うかも知れません。しかし、今、その時代に戻ったとしたら、はたしてどうなるでしょう。社会が動いているスピードは当時とは比較になりませんし、そこには高度な情報流通が欠かせません。現在の経済規模を維持するだけの生産性を得るためには、様々な自動化手段や通信手段は不可欠になっています。そう言う意味で、我々は既にICTにその命運を委ねていると言っても過言ではないのです。

東日本大震災の前、企業のIT部門でBCP（事業継続計画）策定に携わった経験がありますが、災害などでICTが使えない前提でのビジネスは成り立たないということを痛感させられました。災害に対処してビジネスを維持するには、ICTの復旧が不可欠であり、いかにそれらを迅速に復旧するかが、企業IT部門におけるBCPの第一目標なのです。大震災では、電源や通信手段が大きな被害を受け、被災地のビジネスは長期間停止を余儀なくされました。全国規模の大企業はともかく、地場の中小企業にとっては致命的な事態です。

一方、2020年に発生した新型コロナウイルスのパンデミックでは、世界的に人の流れが止まることによる経済への影響が深刻化した一方、ICTの活用やテレワークによって業務を維持した企業も少なくありません。しかし、急激なテレワークへの移行は通信回線や関連する設備に想定外の負荷をかけ、当初、様々な問題が生じました。また、こうしたICT活用への不慣れが原因の問題も多発しています。とりわけ学校のオンライン授業や自治体業務のオンライン化などにおいては多くの課題を残しました。情報セキュリティの面でも、急激な変化はリスクをはらみます。十分なセキュリティ対策を講じる余裕もなく、不慣れな社員にテレワークをさせるという状況が生じ、そこを狙ったフィッシング詐欺やサイバー攻撃が頻発することで、被害も発生しています。しかしながら、こうした経験を経て、社会のICT依存はさらに強まっていくでしょう。

このように、社会やビジネスの基盤がICT化されていくにつれ、それらを狙った犯罪の手段もICT化されていきます。かつて、技術を誇示したい者たち（ハッカー[1]）が、これみよがしに行っていたサイバー攻撃やコンピュータウイルスの技術は、今や企業の情報や消費者の個人情報などを狙った「サイバー犯罪」の手段となりつつあります。旧来からの詐欺の一部は電子メールやフィッシングサイトを使ったものに、窃盗は、電子メールやオンラインバンキングや通販サイトへの不正アクセスを手段としたものにと、次第に変化しつつあります。社会がICT依存を強めれば強めるほど、犯罪者もまたICTを手段として使うようになっていくのです。

このような「悪意あるICT利用者」に備えるためには、新たな「常識」が必要です。現実世界では、犯罪の抑止のために、様々な「常識」が存在します。外出時の戸締まり確認や「鍵」の管理、暗い夜道の一人歩きは避けるといった基本的なものから、ひったくり防止のために、鞄は道路側の手に持たず、自転車のカゴにはネットをかけるといったものなど様々あり、多くが習慣となっています。一方で、ICT活用、すなわち「サイバー」社会での犯罪抑止の方策については、まだまだ常識と言うには、周知が不十分なものが少なくありません。技術やサービスの変化の速さも、その点ではマイナスに働きます。

1…Hacker：一般にはコンピュータシステムの侵害を企てる者の意味で使われるが、インターネットの黎明期においては、高い技術を持つ技術者への敬称として使われた経緯があり、いまだに、この言葉を悪者の意味で使うことに抵抗感を持つ人たちもいる。彼らは悪者のことを「クラッカー」と呼称する。

こうした急速な「サイバー化」の中で、私たちは新たな「常識」を模索していく必要があります。変化の速さに対応するためには、自らリスクを認識し、それを回避する方法を考えることも必要でしょう。単に教えられた「教条」を守るだけではなく、自ら考えて律するという「意識」や「文化」を作り上げていくことが重要なのです。

2. サイバー時代における「人」の価値

「サイバー時代」を象徴するものの一つが、いわゆる人工知能（AI）の発達でしょう。深層学習やニューラルネットワークといった、生物の神経組織の動きをシミュレートするアルゴリズムによって、コンピュータに、より抽象的な課題を解決させることが出来るようになります。既に定型的な問題のほとんどが、コンピュータによる自動化の対象となっていますが、今後は、人の経験や知識、判断に頼るしかなかった作業も、次第にコンピュータ化されていくでしょう。

気の早い人たちは、AIの進化で、人がロボットに支配される‥と言った議論を始めていますが、現在のいわゆるAIは、残念ながら、人どころか動物レベルの知能ですら、まだ置き換えられるものではありません。生物に例えれば、脊髄反射レベルの、知能とすら呼べないものです。SF映画に登場する意識を持つロボットのようなものが実現するには、まだ当分かかりそうです。しかし、いずれは、そんな時代が来るのかも知れません。2045年頃に一大転換点（技術的特異点：シンギュラリティー[2]）が来るという説もありますが、少なくとも、ここ10年程度は、その心配はなさそうです。そうなった時の「人」のあり方は、それまでに考えるとして、今は、現実的な対処を考えて見ましょう。

とはいえ、単純な問題は機械化によって高速かつ確実に解決でき、その適用範囲も次第に拡大していきます。機械と人の（今のところの）最大の違いは、意思を持って行動できることや、知識や経験を抽象化して、**まったく異なる新たな課題の解決に適用**できること（創造性の源泉）だろうと思います。こうした価値を最大化していくことが、これからの「人」が目指すべき方向であり、そのために道具である機械やシステム（ICT）を最大限使いこなす力を身につけることが必要となります。つまり、「考える力」と、ICT技術を使いこなす「スキル」の両面で、自らを高めていくことが重要なのです。

企業、組織における人材の育成においても、こうした要素が欠かせません。手順書的な教育を改め、指針を示すだけで、自ら考えて問題を解決していくことができるような能力を、どのように育成していくかという視点をさらに強化していくことが必要です。これは、ビジネスの上流を担う人たちだけに限りません。日本の製造業が得意とする「カイゼン」活動は、まさにそうした考え方の典型と言えるでしょう。デスクワークの現場においても、これまで以上に、こうした考え方が重要になります。むしろ、現場で、こうした能力が必要とされる時代が来るのです。

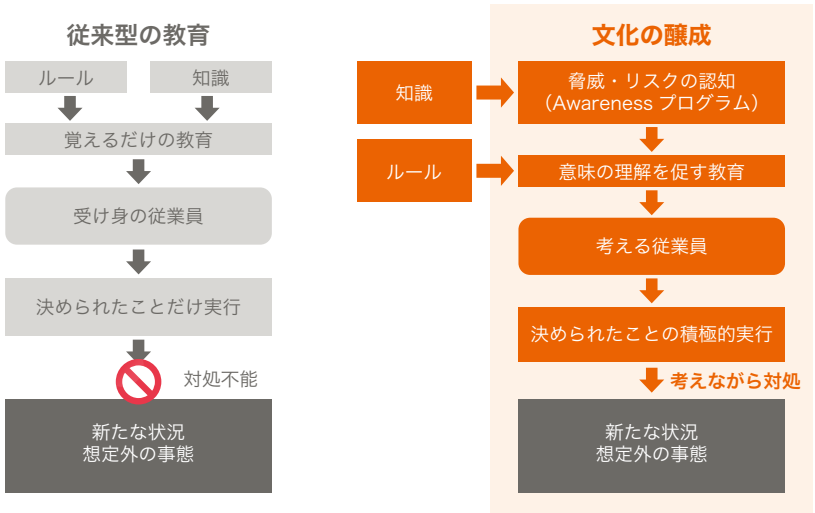
ICT活用におけるセキュリティ上のリスクの認識や対処に関しても、まったく同じ事が言えます。創造的な仕事には一定の自由度が必要です。新たに生み出される状況にルールやマニュアルはありません。社員がそうした領域に踏み出すことを求めるのであれば、自らリスクを認識し回避できる能力をつけさせることが重要となります。もちろん、最低限の基本ルールは必要ですが、それらはより抽象的なものとなり、セキュリティに関する教育はルールの暗唱ではなく、その目的、意図

2‥‥人工知能研究の世界的権威であるレイ・カーツワイルが提唱した。2045年頃にはコンピュータが真の意味での知能を持ち、自己を向上、再生産することにより、技術的な進歩が爆発的に加速し、その先の予測がまったくつかなくなるという考え方。ブラックホールの先が見通せないことに例えて「特異点：シンギュラリティー」という言葉が使われている。

といった本質を教える内容に変わっていく必要があります。その上で、ビジネスの基本である「ホウレンソウ」を前提に、組織としてのガバナンスを保っていくことが重要です。セキュリティリスクの認識（Awareness）を向上させ、自らそれに取り組む「姿勢」や「意識」を組織として醸成し、それらを重視する「文化」を作り上げていくことが、「サイバー」時代の企業に強く求められることなのです。

3. よりよいセキュリティ「文化」を醸成するには

これまでの組織内におけるセキュリティ教育では、ルールの徹底やリテラシーの向上に重点が置かれてきたように思います。もちろん、基本的なルール、業務上の情報やそれを扱うためのシステム、ツールを利用する際の注意点といった事項は、とりあえず直近の業務を安心して進める上で不可欠なものです。しかし、これらをあまりに教条的に捉えてしまえば[3]、様々な弊害が発生します。ある人は、自分の仕事の妨げとなるルールを敢えて無視するかもしれません。一方で、淡々とルールに従って行動し、生産性を全く気にしない人がいる可能性もあります。ルールは一種のテンプレートですが、必ずしもすべてがそれにあてはまるとは限りません。当てはまらない部分があれば、ルールの変更や新たなルール作りが必要となります。しかし、ルール作りにはある程度時間が必要です。一方、その間、仕事を止めてしまえばビジネスチャンスを逃すかもしれません。このような時に、一定のガバナンスをきかせながらも、知恵を絞ってリスクを回避してビジネスを進めることができれば、それは大きな成功に繋がる可能性があります。そのためには、意識と制度の両面での対応が必要です。個々のメンバーが、たとえば新しいビジネスに不可欠なサービスやシステムを利用したいと思った際、ルールが実情に合わないときに、その問題を組織的に提起するという積極性を持つこと。そして、そうした提起を組織的に取り上げて検討し、必要に応じて、当面のガイダンスを発行してビジネスを先に進める制度的な枠組みを作ることです。とりわけ、前者、つまり組織のメンバーの積極性や意識が欠落した場合、先に述べたように相談なしのルール破りや、漫然とルールにのみ従うような事態が生じます。これらは一種の思考停止です。本来、ある前提があってのテンプレートであるルールを前提が違う状況に無理矢理当てはめようとする、いわゆる「テンプレ」な対応は、思考停止を招きます。ルールを作る側も、それに縛られる側も、常に状況を見ながら改善していくという意識を持たなくてはいけません。セキュリティに限らず、そうしたことを是とする企業文化を育てることが最も重要なことなのです。



3…これを端的に表す言葉として、「セキュリティ原理主義」があります。ルールを金科玉条として、いかなる場合も例外なく厳守すべきとする考え方です。

こうした文化を育てるには、全員が「考える」習慣を作り上げる必要があるでしょう。ルールやガイドラインといった物の本質、つまり、その本来の目的や意味、それが、どのようなリスクに対応するのかを理解し、その必要性を認識するような教育、啓発が重要となります。そうした活動が、メンバー全員のリスク認識（Awareness）を高めることにつながります。そして、その課程で得られるフィードバックをルール自体の改善に活かしていく取り組みも必要です。こうしたサイクルが継続し、意識も制度も改善されていく、それが良い企業文化だろうと思うのです。

4. セキュリティ文化を科学する

良いセキュリティ文化と一言で言っても、それは漠然としています。「文化」の重要性は、多くの組織が認識していますが、その実現は言葉で言うほど簡単ではなく、既にこうした活動に挫折した組織も少なくありません。目指すべきセキュリティ文化がどのようなものであり、その達成度をどのように評価するのかを明らかにすることは極めて重要です。それによって、目指す文化とそこに至る過程や、その進捗を明らかにしていくことが必要なのです。これには科学的なアプローチが必要です。

ここで、興味深い研究を紹介しましょう。セキュリティ意識向上トレーニングのための教育プラットフォームをサービスとして提供している米国**KnowBe4社**の傘下にある企業、**CLTRe社**のセキュリティ文化に関する分析です。

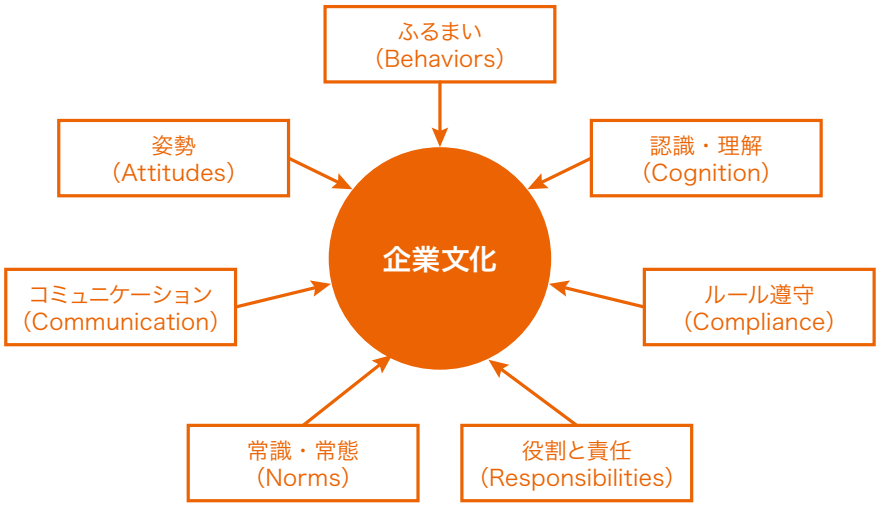
The seven dimensions of security culture（セキュリティ文化における7つの軸）と題する研究レポートでは、セキュリティの文化について、それを構成する7つの要素を定義し、その測定方法に関して論じています。ここでは、その詳細は割愛しますが、以下に要点を紹介しておきます。

彼らは、セキュリティ文化が必要とされる理由について、以下のように述べています。

- **技術的なセキュリティ対策は、他のビジネスプロセスとの調和を保って運用される必要があること。**
- **従業員がセキュリティポリシーと仕事との間で板挟みにならないこと。**
- **セキュリティ意識向上キャンペーンは、それのみでは、進化を続けるサイバー攻撃に対する十分な対策とはならないこと。**
- **組織の「ふるまい」は、従業員が共有している信念や価値観、彼らの行動に依存すること。**
- **従業員を「サイバーセキュリティ最大の弱点」と考えるのではなく、サイバー攻撃に対抗するための「重要な戦力」（人のファイアウォール）とすべきであること。**

さらに、セキュリティ文化は、それ単独では存在し得ず、企業文化の一部として融合されるべきだとも説いています。その上で、セキュリティ文化を構成する7つの軸について、以下のものを挙げています。

1. (仕事やそのセキュリティに対する)姿勢　(Attitudes)
2. (仕事やそのセキュリティにおける)ふるまい　(Behaviors)
3. (リスク、脅威やその対策についての)　認識・理解[4]　(Cognition)
4. (セキュリティに関する様々な)コミュニケーション(Communication)
5. (セキュリティポリシーや標準の[5])遵守状況　(Compliance)
6. (セキュリティにおける)常識・常態　(Norms)
7. (セキュリティに関する)役割と責任　(Responsibilities)



企業文化を構成する７つの軸

これらの軸は、セキュリティだけでなく、企業文化全般を評価する上でも重要なものです。リスクに対する正しい認識と理解が、従業員の姿勢やふるまいを改善し、ルールの遵守や、リスクに対応するためのコミュニケーションを促し、それぞれがその役割に応じて果たすべき責任を正しく認識するという好循環を作り上げ、継続的な向上を実現することこそが、セキュリティ文化の醸成であると彼らは考えているのです。

各軸の評価、測定に関して、彼らは、それぞれに重要と思われる事柄を問うアンケート形式のサーベイを開発しています。各設問は、心理学的な観点から作成され、実際に、使われる言語ごとに数百名規模のテストを行って設問への回答が正しく状況を反映しているかどうかを検証しています。このサーベイは、KnowBe4社の教育プラットフォームに実装され、ユーザに使用されています。

4…単なる「知識」ではなく、「本質的な理解」を意味するとの解説がある。

5…日本では、コンプライアンスは「法令遵守」と訳されることが多いが、英語では、様々なルールの遵守と、より広い意味で使われる。

5. セキュリティ意識向上プログラムの動向

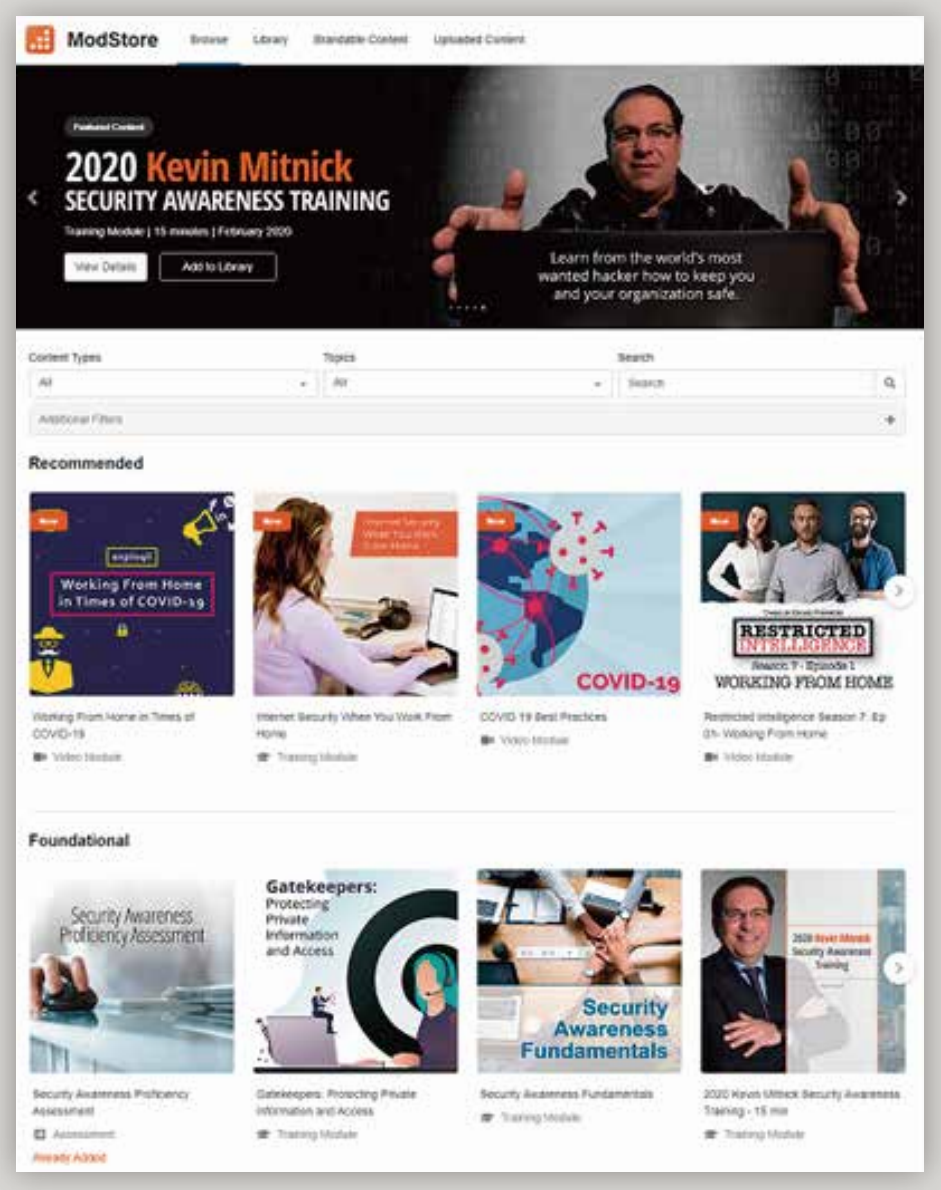
セキュリティ意識向上プログラム（トレーニング・キャンペーン）は、まだ日本国内ではなじみが薄い言葉です。国内企業・組織におけるセキュリティ教育プログラムでは、先にも述べたように、ルールの徹底やリテラシーの向上を目指す知識教育が中心に見えます。一方、欧米企業では、早くから、従業員の意識や認知向上を目的としたプログラム（Awareness Training Program）の開発が盛んに行われており、有名なセキュリティ関連のセミナーやコンファレンスには、必ずAwareness Programに関するセッショントラックが設けられています。集まった参加者からは、様々な現場の課題や悩みが出され、議論が活発に行われています。とりわけ、近年、従業者を標的としたメール攻撃やソーシャルエンジニアリングと呼ばれる詐欺的手法を駆使した攻撃により、コンピュータウイルス（マルウエア）感染や、パスワードの漏洩といった事態も増加しており、その手口も日々高度化しています。こうした状況に対応するため、従来型の単なる啓発教育ではなく、先に述べたような防御における「従業者の戦力化」のための教育への移行が急がれているのです。

最近、こうしたコンファレンスに参加していて、興味深いと感じたのが、講師や参加者の何人かが、「Awareness Programは社内マーケティング活動だ」と述べていたことです。いかにして、従業員の興味を引き、退屈させずに、彼らの意識を高めるコンテンツを作るか、という点がマーケティングそのものだと言うのです。ある企業では、Awareness Programを担当する部署にマーケティング部門から人を招いて成功を収めた事例もありました。受講者がリスクを自分の事として認識し、意識を変えていくためには、単に知識を詰め込むだけでなく、脅威やリスクを肌で感じて貰えるようなコンテンツ作りが欠かせないのです。

最近では、従来から使われてきたスライドベースのEラーニングコンテンツではなく、ストーリーのあるドラマやコント形式の動画コンテンツが多用されはじめています。日本でも、**IPA（情報処理推進機構）**などが、動画形式のコンテンツを多数公開するなど、受け手に訴えかけるコンテンツ作りが始まっています。スライド形式のコンテンツにおいても、様々な工夫が行われ、一部に動画を入れたり、クイズや簡単なゲームを入れたりと、次第に内容も様変わりをはじめています。

しかし、こうしたコンテンツを各企業が独自で開発するのは大変です。前述したIPAのコンテンツなどを利用することも可能ですが、社員の受講を管理したり、理解状況を評価したりするためには、ラーニングシステムを導入する必要があります。こうした問題を解決するためには、クラウド上から提供されるラーニングサービスなどを利用するのがよい方法でしょう。ひとつの例が、先に挙げたKnowBe4社のサービスです。同社は動画のドラマ形式を含む様々なトレーニングコンテンツや、フィッシング（標的型メール）訓練のためのプラットフォームなどを統合し、それらや利用者独自のEラーニングやビデオコンテンツも利用した総合的な「意識向上プログラム」を計画、実施できるプラットフォームサービスです。また、同社は、「伝説のハッカー」であり、ソーシャルエンジニアリングの大家でもある、ケビン・ミトニック氏をアドバイザーに迎え、彼の監修により、様々な攻撃に耐性をつけるためのコンテンツを充実させています。こうしたサービスの利用も、意識向上や文化育成を効率的に行う良い方法でしょう。

KnowBe4社が提供するコンテンツの例



著者紹介

二木真明　（ふたぎ　まさあき）

アルテア・セキュリティ・コンサルティング（個人事業）　代表

1956年生まれ

17年間の制御系やUNIXシステムプログラマー、SEとしてのキャリアの中で、ファイアウォール製品を開発し、商品化したことから情報セキュリティの世界に踏み込む。その後、現在まで25年近く、情報セキュリティの様々な分野で経験を積んだ。2000年以降は、大手商社系SIerに勤務し、海外セキュリティ製品の発掘や技術評価などにたずさわる一方で、自社内の情報システム部を兼務し、様々なセキュリティ対策の導入やルール整備、社内SOCの業務等を主導した。2012年に独立して、その後は経験を活かして、主にユーザサイドの様々なセキュリティ案件の支援や社内教育サポート、セキュリティベンダーの製品開拓、立ち上げのアドバイスなどを行っている。

CISSP: (ISC)2認定情報システムセキュリティプロフェッショナル
CISA: ISACA認定情報システム監査人

その他経歴など

2014年4月～2017年3月　埼玉県警察サイバー犯罪対策技術顧問
CSAジャパン（日本クラウドセキュリティアライアンス）運営委員
同IoT ワーキンググループリーダー
JNSA（NPO 日本ネットワークセキュリティ協会）幹事
株式会社　電通国際情報サービス　金融システム事業部　セキュリティ戦略アドバイザー

主な執筆書籍：

IT管理者のための情報セキュリティガイド　インプレス Next Publishing

【共著】

IoTセキュリティ　日経BP社　　（3-3 IoTシステムのリスク評価を考える）
APT対策入門　日本セキュリティ監査協会編　インプレス Next Publishing

その他、Web等、執筆記事多数

株式会社電通国際情報サービス（略称 ISID）
金融ソリューション事業部　戦略アライアンス部

〒108-0075 東京都港区港南2-17-1
紹介URL：https://www.isid-security.com/knowbe4/
E-mail：g-security@group.isid.co.jp
Tel：03-6713-7030

本ソリューションの
詳細情報はこちら