AIG

Cyber

# ヒトサイバーリスク
## ― 防御の第一線

AIG損保

**サイバーリスクに関するエッセイや記事では、人為的ミスがサイバー事故とそれによる金銭的損失の主な原因であると言及されていることが多く、全セキュリティ侵害の最大 95% を占めている[1]。しかし、ヒューマンエラーとは何であり、悪意ある行為者により人間の特性や行動がどのように利用されてしまうのだろうか。これらの脆弱性をよりよく理解することで、これらの脆弱性に対処し、より大きなサイバーレジリエンスを構築するために、より多くのことを行うことができる。**

本報告書は、エンドユーザーとインフラがハッカーと詐欺師によって利用される一連のシナリオを考慮して、サイバー脆弱性に関連する人的要因を検討します。様々なタイプの人間の脆弱性を考慮し、より良い認識とトレーニングとより堅牢な IT インフラによって、脆弱性をどのように低減できるかを検討します。

世界的な新型コロナウィルスの大流行を背景に、従業員がリモートで作業している場合に企業が直面する追加的なリスクについても検討します。危機的な状況では、従業員はパッチが適用されていない古いデバイスやソフトウェアに頼らざるを得なくなり、本来の恐怖心を悪用した詐欺にさらされる可能性が高くなります。

本報告書では、従業員がミスを犯したことを非難するのではなく、根本的な原因である人間の行動を特定し対処することによって、サイバーリスクの人間的側面に対処する新たなアプローチを取るべきだと主張しています。これは、主に感情的な脅威のニュアンスをすべて認識し、推奨と解決策を提供するアプローチですが、ユーザーを犯人として非難することではありません。

私たちはヒューマンエラーという言葉を人的要因に置き換え、否定的な意味合いから脱却するとともに、組織に対して脅威に加えて機会を特定するための余地を与えます。企業は、セキュリティ管理やその他のインフラによるITシステムの保護に多額の投資を行っており、2020年には投資額は420億ドルを超えると見込まれています[2]。しかし、企業の世界では、データとシステムの保護に関しては、社員が第一線に立つことを保証するために、必要なだけの投資を行っているのでしょうか。

**キーポイント**

- ヒューマンエラーとは、サイバー攻撃の責任は人にあるという意味だ。実際には、不十分なセキュリティカルチャーが人間中心の攻撃を助長している。
- ソーシャルエンジニアリング攻撃の焦点は、より的を絞ったものになりつつあり、十分なアクセス権と特権を持つ人々を危険に陥れようとしている。
- 在宅勤務が増加している現在、個人はこれまで以上に悪意のある人物による攻撃に対して脆弱になっている。

**覚えておくべきこと：**

- **注意：**サイバーリスクを定期的に評価し、影響と予算に基づいてアクションの優先順位を決定する。
- **率先：**セキュリティの基本を覚え、脆弱性率先してテストを行う。
- **準備：**システム障害の対応計画を策定し、従業員の準備を行い、代替案を事前に決定しておく。

[1] https://blog.getusecure.com/post/the-role-of-human-error-in-successful-cyber-security-breaches
[2] https://www.weforum.org/agenda/2019/07/can-cybersecurity-offer-value-for-money/

# 人的要因とは何か？

人的要因は、実際のミスというよりも、不適切なセキュリティカルチャーや人間の行動や善意の悪用と関係しています。人間が職場でどのように行動し、悪意のある行為者がどのように古典的な人間の特性を利用しようとしているかをよりよく理解することによって、人間の誤りやすさの領域を特定し、対処することが可能になります。

標的型攻撃では、上級管理職や中間管理職は、下級管理職よりもサイバー犯罪者にターゲットにされる可能性が高いです[3]。これは、重要な情報を保持する傾向があること、およびそのようなデータにアクセスする可能性が高い傾向があるためです。経営幹部がソーシャルエンジニアリングのターゲットになる可能性は、数年前に比べて９倍になっています[4]。

**図1：AIG EMEA (2018) から受けたサイバー請求 – 情報源は報告された事故**


＊ サービス拒否攻撃、データプライバシー規制違反に基づく法的手続き

## ソーシャルエンジニアリングとビジネスEメールの侵害

ソーシャルエンジニアリングとは、個人をだましたり、誘惑したり、脅したり、脅迫したりして、個人情報や企業情報を提供させたり、支払いをさせようとすることです。Eメールは、悪意のあるスパムから、企業のEメールを悪用した攻撃（BEC：Business E-mail Compromise）に至るまで、依然としてソーシャルエンジニアリングの主要な攻撃対象となっています。このような方法は、必要なハッキングの専門知識が最小限で済み攻撃の成功率が高いため、一般的です。

BECの加害者は、企業のCFOなど、支払いの送信に責任のある個人を標的にすることが多いです。ソーシャルエンジニアリングを通じて、ユーザーが情報を提供したり、金銭取引をすることを促すために心理学的操作を行います。ソーシャルエンジニアリングには、架空の請求書を買掛金処理チームに送るなど、好奇心を刺激するように設計された単純なルアーから、より精巧なスキームまで、様々なアプローチがあります。

攻撃者は盗んだブランドを使って、一見合法的に見えるランディングページやドメインを作るかもしれません。これらのテクニックは、BEC攻撃で使用されます。この攻撃では、脅威の主体が、信頼できる企業と通信しており、CEO、同僚、ビジネスパートナー、またはサポートスタッフのふりをしていることを被害者に納得させようとします。

[3] https://www.cio.com/article/3247428/safeguarding-your-biggest-cybersecurity-target-executives.html
[4] https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf

2019年の AIG EMEA Cyber Claims Intelligence Report によると、BEC はサイバー保険請求の主要な推進力として、ハッカーによるランサムウェアとデータ侵害を上回っています。2018 年に AIG に報告された事件のほぼ 4 分の 1 は、BEC から生じた損失によるものであり、企業の幹部でさえこれらの詐欺の犠牲になったという事例証拠があります。全世界で、企業は過去三年間に BEC に推定 260 億ドルの損失を出しています[5]。

AIG ヨーロッパのサイバーリスクアドバイザーである Sebastian Hess 氏が説明するように、その理由の 1 つは、ソーシャルエンジニアリングの利用です。専門家の目から見ても合法的に見える電子メールを作成しています。

「ソーシャルエンジニアリングは依然として最大の脅威の 1 つであり、従業員や上級管理職を標的にしたセキュリティインシデントを引き起こしている。」と彼は言及します。「新しいトレンドには、ソーシャルエンジニアリング技術を利用して重要なデータやお金を盗む電子メール詐欺がある。これらの攻撃はますます巧妙になっており、攻撃者は手段を強化し、セキュリティに対抗する方法を見つけている。」

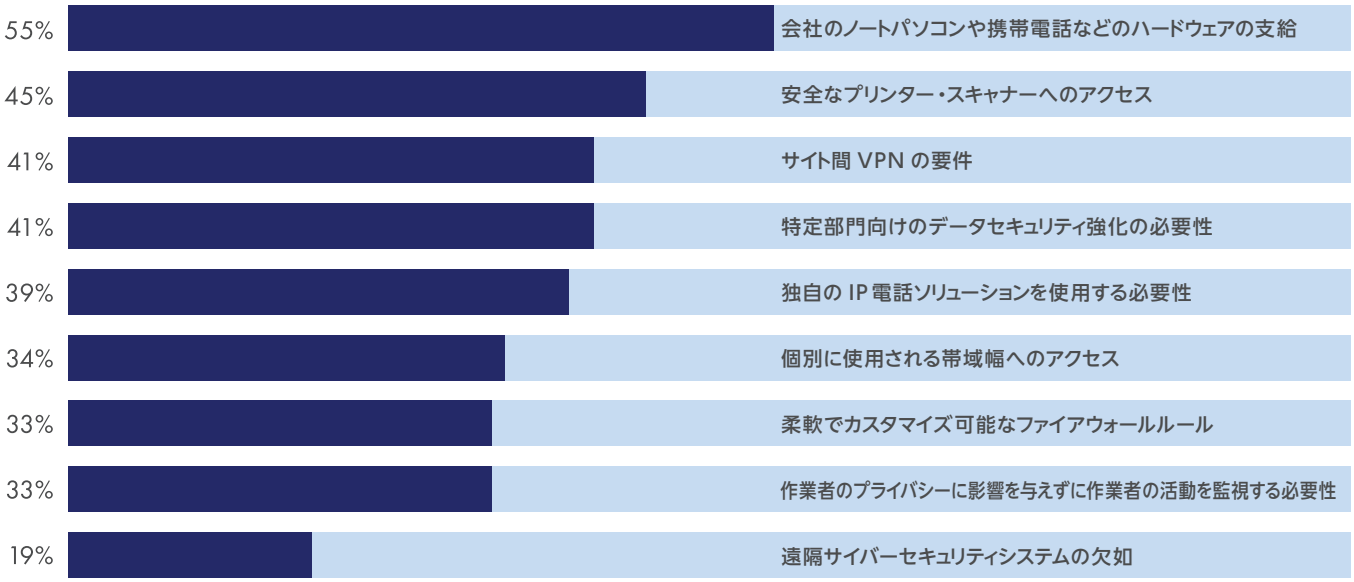
## 在宅勤務／隔離ストレス

世界中で、企業は隔離や社会的距離の制限の中で、在宅勤務の現実の高まりに直面しています。緊急のビジネス継続性計画を策定する際、従業員はサイバー脅威にさらされます。困難な状況で最善を尽くす従業員は、多くの場合、セキュリティの低い個人用デバイスに頼らざるを得なくなりますが、その一方で、ストレスレベルが高まると、攻撃を受けやすくなる可能性があります。

在宅勤務の増加は、従業員が悪意ある行為者に搾取されるリスクを必然的に高めます。現在、政府が自宅隔離制限を課しているためにこれらのリスクが表面化してきていますが、企業がデジタル化と新しい働き方を取り入れていることから、このような露出はより大きな変化の一部です。

在宅勤務に関連するビジネス上の課題の中には、データセキュリティに関する懸念や、生産的に働くために必要なすべての技術を労働者が利用できるようにすることに関する懸念があります。平時においては、企業は柔軟な働き方を導入または拡張したり、BYOD (Bring Your Own Device) ポリシーを設定したりする際に、自社の技術的要件を慎重に検討できますが、緊急時には簡単にはできません。

**図 2：企業が柔軟な働き方を導入・拡大する際に考慮する技術要件**




出典：International Workplace Group

[5] https://www.securityweek.com/loss-bec-fraud-now-claimed-be-26-billion

スタッフが突然リモートでの作業を強いられた場合は、自宅のコンピュータやその他の個人用デバイスを使用する必要があります。サプライチェーンの混乱の中でPCの需要が増大すると、企業が従業員に提供できるノートパソコンやその他のデバイスが不足する可能性があります。

個人用デバイスは職場での保護と同じ保護を受けている可能性は低く、活動を監視する能力も同じである可能性は低いです。したがって、企業はITセキュリティの高い標準を維持し、従業員が個人用デバイスの安全性を確保できるよう支援する必要があります。

さらに、企業はリモート接続を可能にする新機能を導入しています。例えば、従業員の在宅勤務を可能にするリモートデスクトッププロトコル（RDP）が挙げられます。しかし、セキュリティ上の検討事項にこのサービスの導入は含まれていたでしょうか?アクセスは適切に保護されていますでしょうか?

雇用者とそのスタッフは、これらの詐欺や日常的なサイバーセキュリティの落とし穴に注意を払うべきであり、例えばスタッフが二要素認証と強力なパスワードを使い続けられるようにしなければなりません。従業員には、サイバーセキュリティの観点から何に注意すべきか、また、フィッシングEメールのリンクをうっかりクリックしたり、サイバー攻撃の標的にされたと疑われたりした場合にどうすべきかについて、定期的に注意を喚起するメッセージを送るべきです。

## 注意散漫とモバイルデバイス

Verizon社によると、モバイル端末のユーザーは、デスクトップのユーザーよりもフィッシングやソーシャルメディア攻撃、なりすまし（正規のウェブページを模倣しようとする）の影響を受けやすいといいます。これは、モバイルデバイスのデザインとユーザーの操作方法に起因します。

画面サイズが比較的限られていると、アクセスや表示が明確に制限され、アプリが情報の可用性を制限することが多く、メールやリクエストの正確さをチェックするのが難しくなります。モバイルデバイスはまた、個人が歩いたり、話したり、その他の活動をしているときにもよく使用され、注意力が散漫になる可能性があります。タブレットやスマートフォンなどのモバイルデバイスに関連するリスクは、多数のスタッフがリモートで作業している場合には、企業にとって明らかに大きな問題となります。

## 無意識かつ自動的な行動

エンドユーザーのリスクに関しては、助けになりたいという自然な欲求など、より柔軟な要因が数多く働いています。多くの点で、サイバー犯罪は、恐喝・詐欺など、より伝統的な犯罪の進化形です。活動の規模は拡大しておりますが、詐欺や操作には同じような手法が用いられています。

心理学的な観点から見ると、思いやりのある行動に参加することは、報酬系に関連する脳の部分を活性化し、肯定的な感情と利他的な行動を強化します。それはヒューマンエラーという言葉が暗示するように、人がミスをすることだけではありません。大規模で洗練された企業は、サイバー脅威に対する技術的障害の開発に多大なリソースを費やしていますが、人間行動の観点からは十分な効果を発揮していますか。

トレーニングと自覚が高まっています。Verizon 社の調査[6]によると、今日の従業員がフィッシング攻撃に引っかかる可能性は、7年前より低く、24%から3%に低下しました。しかし、特にフィッシングメールがより説得力を持つようになってきたことを受けて、人々は依然としてすべきでないリンクをクリックしています。

**サイバーセキュリティのベストプラクティスを遵守しない理由**（出典：英国政府科学局）

- 多くの場合、接続の必要性は、安全でない接続のリスクを上回る。
- 人々は「同意する」ボタンと警告メッセージに慣れている。
- 便利さはセキュリティよりも常に勝る。
- 知覚される利益はない － 行動がセキュリティに影響を与えないという信念。
- 知識とスキルの不足：何をどのようにして行うかに関する知識、不正行為を検出するためのスキル。
- オンラインで他のことに気を取られているときに、安全に行動することを忘れてしまうだけ。

リンクをクリックするなど、人間の行動はある程度自動化されます。ユーザーがウェブページにアクセスするなどの行動をしたときに、期待していたものを得ることで「報酬」を得るとすれば、こうした繰り返しの行動は、無意識のうちに行われているため、さらに困難になります。ユーザーがサイバーセキュリティのベストプラクティスに従わない可能性がある行動上の理由は数多く存在します（【左下：サイバーセキュリティのベストプラクティスを順守しない理由】参照）。

心理学では、手順記憶とは、歩行、会話、運動能力や習慣の習得など、特定の機能をどのように遂行するかについての情報を保存する一種の潜在記憶のことです。手続き的記憶を通して、ユーザーは「I accept(同意する)」ボタンや、例えばウェブサイト上の GDPR クッキー警告に慣れ、自然にボタンをクリックしてしまいます。

**パスワードの衛生状態がどのように進化したか**

不十分なパスワードの衛生状態の問題は解消されていませんが、ベスト・プラクティス・アプローチは進化しています。単純なパスワードは、通常、セキュリティで保護されたネットワークで最も弱いリンクです。多くの場合、攻撃者はパスワード解読ツールを使用して、暗号化されたパスワードを回避し、ユーザーのアカウントにアクセスします。パスワードが「password」、「qwerty」「1234567」などの単純なものである場合は、この方法の方が簡単です。2014 年に発生した iCloud のセキュリティ侵害では、攻撃者が多数の有名人の個人的な写真にアクセスしていたが、このような強引な手法が背景にありました。

以前は定期的にパスワードを変更するように勧められていましたが、現在では、強力なパスワードを設定し、それを使い続ける方が便利だと考えられています。National Institute of Standards and Frameworks（NIST）では、最低でも 8 文字の長さのパスワードを推奨しています。また、覚えやすい単語やパスフレーズを含む非常に長いパスワードも推奨しています。複雑なパスワードを使用しないようにアドバイスします。

ガイドラインが最後に修正された 2017年には、NISTは、ユーザーが数か月ごとにパスワードを変更することを要求するリセットを削除することも推奨しました。また、パスワードの強さは、量ではなく質であるべきだと主張しました。

[6] https://enterprise.verizon.com/resources/reports/dbir/


### ソーシャルエンジニアリング – データが多すぎて時間がない

ソーシャルエンジニアリングの背後にある考え方は、潜在的な犠牲者の自然な傾向や、同僚を助けたいという従業員の欲求などの感情的な反応を利用することです。犯罪者は、差し迫った期限などのプレッシャーのかかった状況を作りながら、信頼を得るために同僚のふりをして、個人が「先に行動し、後から考える」ようにするかもしれません。

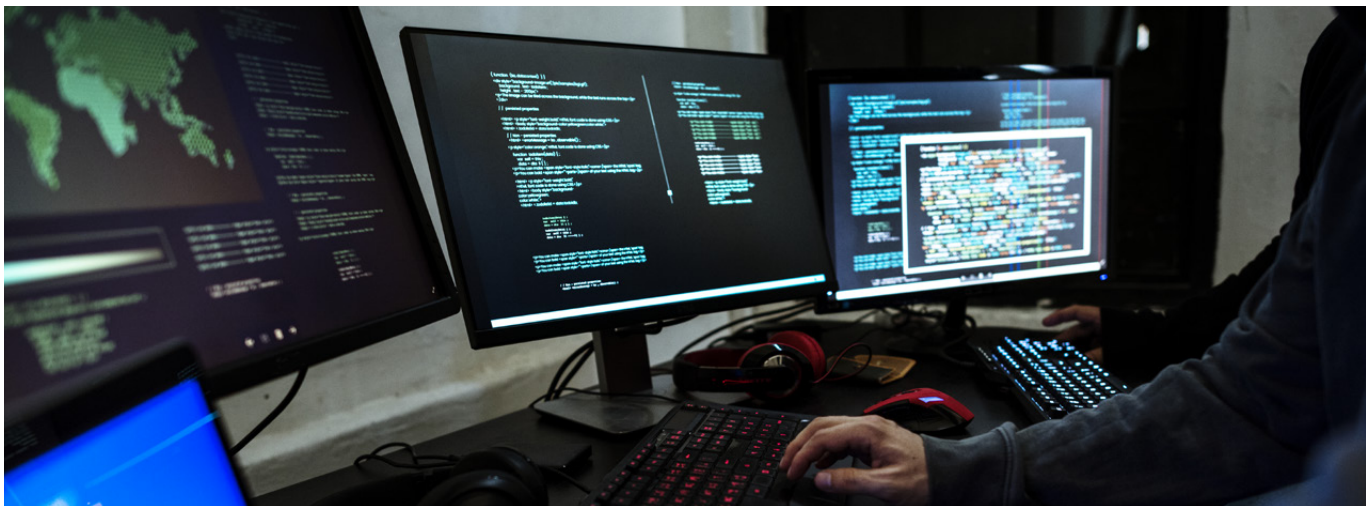
ソーシャルエンジニアリング攻撃の種類には、ベイト、フィッシング、E メールハッキング、スパム、および vishing（電話で行われるフィッシングと同じ詐欺）が含まれます。被害者の名誉を傷付けるような映像や画像を友人や家族に公開するように言われるセクストーションも、ソーシャルエンジニアリングと根は同じです。

ソーシャルエンジニアリングはオンラインとオフラインの両方で行われており、詐欺師たちはソーシャルメディアのアカウントを通じて収集されたデータを含むあらゆる種類の情報を利用して、自分たちが本物であるかのように見せかけています。

ウイルス対策ソフトウェアを提供しているNorton社[7]は、ソーシャルエンジニアリングの犠牲にならないように、以下のヒントを推奨しています。

- ソースを検討する。見つかった USB スティックは必ずしも良いものではなく、マルウェアが仕込まれている可能性がある。今日では、すべてのメール送信元が疑わしいと考えられている。
- スピードを落として。ソーシャル・エンジニアは、要求が本物かどうかを考慮せずに、ターゲットが迅速に行動することを期待する。どんなに仕事量が多くても、立ち止まって考えたり質問をしましょう。
- 話がうますぎて本当とは思えない。ナイジェリアの王子が助けを求めてる可能性はどれくらいありますか？金銭または個人情報の要求があった場合は、それを引き渡す前に調査する。
- 最新のセキュリティ脅威に対応できるように、オペレーティングシステムをアップデートしてパッチを適用する。
- 電子メールソフトウェアを使用して、詐欺を含む迷惑メールを除外する。

[7] https://us.norton.com/internetsecurity-emerging-threats-what-is-social-engineering.html



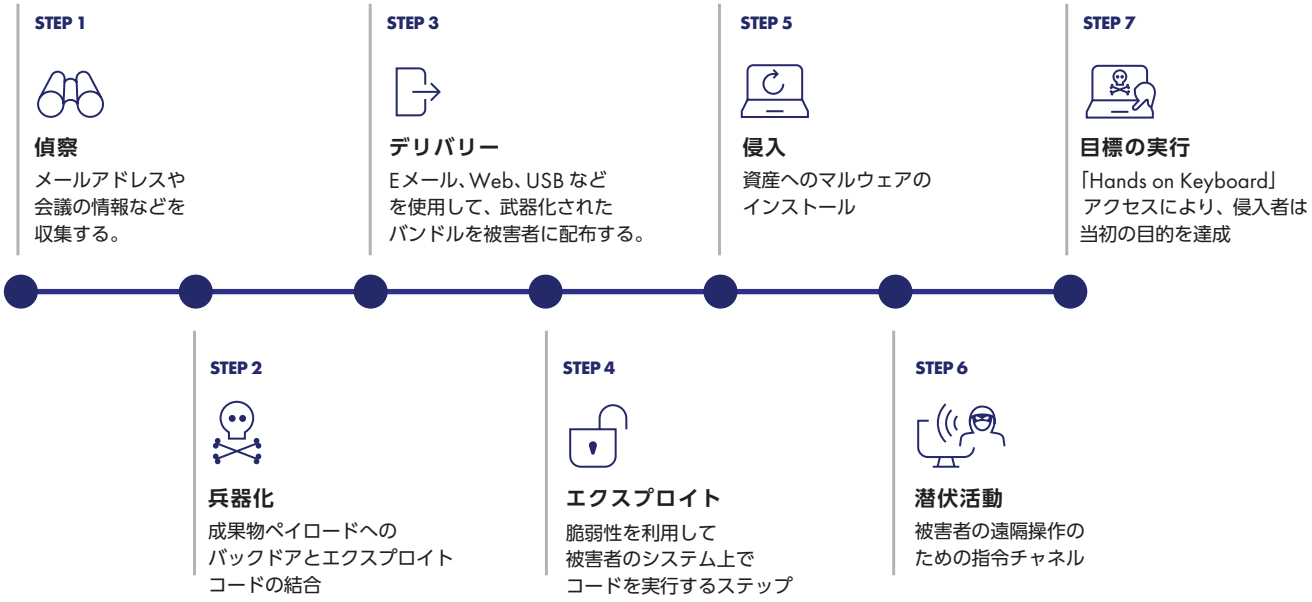
## サイバー犯罪者とそのマインドゲーム

様々なタイプのサイバー攻撃者とその特性を理解することは、企業が潜在的な脅威をより的確に特定するための要員の準備に役立ちます。国民国家主体から社会政治的ハクティビストまで、攻撃者の動機は様々です。しかし、その影響は、NotPetya攻撃の場合のように、実際の標的よりもはるかに広範囲に及ぶ可能性があります。

サイバー犯罪者は通常、金銭的な利益を目的としており、必要なものを簡単に抽出する方法を求めています。組織化された組織の一部であることが多く、高いモチベーションと高度なスキルを持ち、時間と資源が無制限です。彼らは心理戦をするのが大好きです[8]。企業ネットワークに侵入するために必要な情報を入手するために電話を取り、オフィシャル・サポートやテクニカル・サポートになりすますのは、力ずくのハッキングに何ヶ月も費やすよりも簡単です。

サイバーキルチェーンとは、サイバー犯罪者が初期の偵察段階からデータの浸透に至るまでにとる一連の手段のことです。企業がランサムウェア、セキュリティ侵害、その他の攻撃に対処しようとする際、人的要因は、キルチェーンを中断させる重要な要素です。

図3:Lockheed Martinのサイバーキルチェーンの方法論 – 人間がどのように防御の最前線にいるか




[8] https://home.kpmg/uk/en/home/insights/2018/07/mind-games-how-to-protect-your-business-against-cyber-crime.html

# 自分を自分から守る

サイバーの人的要因に対処することは、堅牢なサイバー・セキュリティー・フレームワークを導入するための企業全体のアプローチの重要な部分です。成功は、次のような日常的な小さな行動によってもたらされます。

- インシデント対応機能
- ネットワークセキュリティの原則
- セキュリティ意識向上トレーニング
- 率先的なセキュリティテスト
- パッチ管理プログラム
- 安全なデータバックアップ

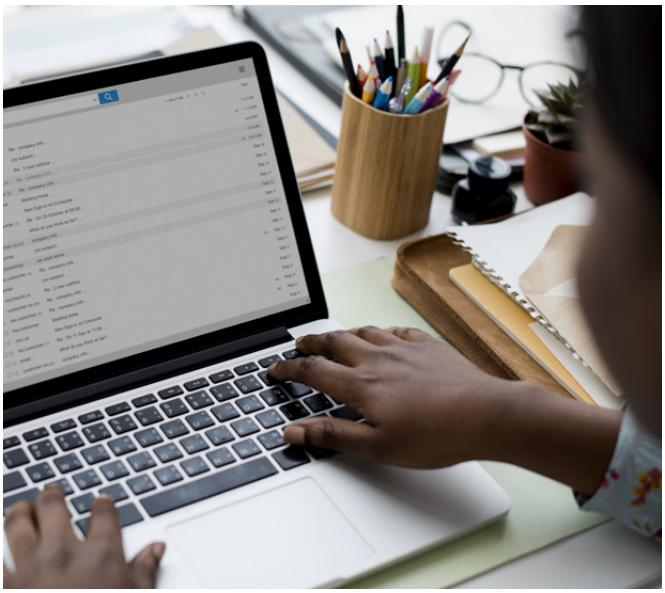
雇用者は、サイバー犯罪者が人間の行動を利用して従業員を騙し、リンクをクリックさせたり、パスワードを渡したりする際に利用する心理的レバーを考慮する必要があります。例としては、善意、不注意・失効・急いでいること・信頼しすぎていること、原則などがあります[9]。これらの特性がどのように悪用されているかを理解することにより、スタッフに事前警告を行い、二要素認証または多要素認証のようなセキュリティプロトコルを実装して、これらの傾向を無効にすることが可能です。

サイバー脅威との戦いが続く中、企業は ヒューマンエラーという言葉を捨て、従業員のセキュリティを強化する方法を検討する必要があります。Usecure（英国発の著名なセキュリティ関連のブログ）のブロガー Micke Ahola 氏が説明しているように、「知識の不足はユーザーの責任ではないが、企業が対処すべきである」[10]。したがって、エンドユーザーが自分自身とビジネスを安全に保つために必要な知識とスキルを備えていることを保証する一義的な責任は、雇用者にあると考えられています。

従業員は、研修、ミーティング、ゲストスピーカー、部門横断的なチーム、テスト、内部リソース、および毎週の更新などの形式で定期的なトレーニングを受けることで、より適切なセキュリティの選択を行うことができます。ゲーミフィケーションは、雇用主がサイバーセキュリティのトレーニングにスタッフをより積極的に参加させるために用いている戦略の1つです。ここでは、経営幹部が 実演シミュレーションに参加して、学習を促進する楽しい方法で意識を向上させ、良い習慣を身につけることができます。

もう 1 つの戦略は、従業員を定期的に倫理的なハッキング攻撃にさらすことで、彼らのペースを落とすことです。火災が発生した場合の正しい避難手順を誰もが覚えているように、模擬フィッシング攻撃では、不審な E メールを見つけて仮想環境で安全に保管するスタッフの能力をテストできます。従業員がシミュレートされたフィッシング詐欺を体験できるようにすることで、リスクの認識が高まり、今後の E メールに疑念を抱く可能性が高くなります。

行動科学はサイバーリスクに関連する人的要因をより良く理解するためにますます利用されています。MINDSPACE フレームワークは、公共政策を用いた成功した行動変化介入の設計を支援するために、財政・健康的な食事・持続可能性を含む多くの背景で成功裏に使用されてきました。このようなアプローチを用いることで、ユーザーが無意識のうちに正しい選択をするように影響され、例えば、安全でないサイトがより目立つようにユーザーを積極的に妨害することができます。



[9] https://theconversation.com/five-psychological-reasons-why-people-fall-for-scams-and-how-to-avoid-them-102421

[10] https://blog.getusecure.com/post/the-role-of-human-error-in-successful-cyber-security-breaches

## 必要最小限の特権

優れたセキュリティもまた、ツールキットの重要な部分です。重要な情報資産を保護する役割を果たすようにユーザーをトレーニングすることは、企業が必要とするアプローチの1つです。もう1つは、より脆弱なユーザーを保護することです。これは、ファイアウォール、ウイルス対策ソフトウェア、パッチ、強力なパスワード、およびその他の基本的なセキュリティソリューションを重視した強力なセキュリティプログラムによって実現できます。

セキュリティ方針と手続きは、回復力のある防衛の大きな要素です。多要素認証、バディシステム 、およびユーザー権限の管理により、ミスが発生する可能性が低くなり、内部者からの脅威を最小限に抑え、アカウントが危険にさらされた場合の全体的な影響を抑えることができます。

多要素認証のベストプラクティスには、通常次のものが含まれます。

- **知識要因**とは、パスワード、PIN、またはその他の種類の共有シークレットなど、ユーザーが知っている。
- **所有要因**とは、IDカード、セキュリティトークン、スマートフォン、その他のモバイルデバイスなど、ユーザーが持っている。
- **生体要素**は、より一般的にはバイオメトリクス要素と呼ばれ、指紋リーダまたは顔および音声認識によって認証される指紋など、ユーザーの身体的自己に固有のもの。
- 通常、認証試行が行われている位置によって示される**位置要素**は、認証試行を特定の装置、IPアドレスまたはGPSデータに制限することによって実施することができる。
- **時間係数**は、ユーザー認証をログオンが許可される特定の時間枠に制限し、その時間枠の外でシステムへのアクセスを制限する。

英国のNational Cyber Security Centreは、ユーザーに不要なデータアクセス権を与えることを警告し、高度化されたシステム権限の付与は慎重に制御および管理することを推奨しています[11]。

「高度な権限を持つ管理アカウントは、Webブラウジングや Eメールなど、高リスクの日常的なユーザーアクティビティには使用しないでください。」と言及します。「ユーザーアクティビティを監視してください。特に機密情報へのアクセスでアクティビティが予期される範囲外にある場合は対応してください。」

Ponemon Institute社の調査によると、AIと機械学習には役割があり、企業のほぼ4分の1が「サイバー攻撃やサイバー侵害の特定と封じ込めへの人間の介入を強化する、あるいは置き換える」セキュリティ技術をすでに使用しているといいます。高度に自動化された企業の方が、セキュリティインシデントやITおよびビジネスプロセスの中断を防ぐことができます。

堅牢なサイバーセキュリティプログラムを提供するためには、異なる部門が協力してサイバー脅威からスタッフを保護することが重要です。サイバーセキュリティは従来、IT部門やCISOの仕事と考えられてきましたが、脅威の変化に伴い、経営幹部・人事・リスク・保険の専門家などを巻き込んだ戦略的な全社的課題となっています。

「サイバー犯罪者はよりソフトな標的に向かい、人間の行動や脳の働きを利用した攻撃を実行している。」とAIGのEMEAサイバーヘッド、Mark Camillo氏は言及します。「組織化された犯罪集団は、最も簡単に、そして現在、ビジネスEメールの侵害で最も儲けることを可能にする戦術を使っています。明らかに、詐欺師がどのように会社の資金を盗んだり流用したりしているかを理解するには、より全体的なアプローチが必要である。」

[11] https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security?curPage=/collection/10-steps-to-cyber-security/the-10-steps/managing-user-privileges

フィッシングメールを識別し、パスワードを改善し、セキュリティ保護されていないデバイスからネットワークを保護するためのスタッフのトレーニングなど、内部の脅威の管理には時間とリソースがかかります。サイバーセキュリティ部門は、ユーザーをサイバーセキュリティ戦略の中心に据え、様々な業種からの賛同と参加を得ることで、時間を解放して外部からの脅威の管理に集中し、企業全体のサイバーセキュリティに対してより戦略的なアプローチをとることができます。

**サイバーセキュリティのための**

- 同じパスワードを再利用しない
- 複雑なパスワードを使用する
  （雇用者はあらかじめ決められたパスワード強度を要求すべき）
- パスワード保管庫を利用する
- 多要素認証を有効にする
- 雇用主のネットワークに接続しているときは、個人アカウントにアクセスしない
- 仕事に関連する作業を行う前に VPN 経由で接続する
- オンラインアクティビティへのフィルタリングメジャーの適用
- サイバーセキュリティ研修の充実

## まとめ

最も洗練された企業群の IT システムでさえ、侵害される可能性があるという認識があります。彼らが失敗するのは彼らの技術ではなく、彼らの人々を守るために導入されたフレームワークとシステム（もしくはその欠如）であることがあまりにも多いです。

人間は自然と、ラインマネージャーや同僚を喜ばせ、仕事をやり遂げるためにスピードを求めますが、それによりセキュリティプロセス、特に生産性、職場の満足度、利便性に反するように見える対策を見落としがちです。しかし、企業が従業員の保護に成功するためには、バランスを保つ必要があります。

ヒューマンエラーという単純なキャッチフレーズを超えて、エンドユーザーが直面している重大な脆弱性を企業が理解し、対処する時が来ています。これは、サイバー攻撃の機会を減らし、企業文化を改善し、従業員により良い知識と訓練を与えることを意味します。

サイバー脅威の状況が増大し、進化するにつれ、最も回復力のある企業は、技術と行動の両方のレベルで脅威に取り組み、企業全体で協力し、あらゆるレベルで賛同している企業です。あらゆる企業のサイバーセキュリティ文化の基調は、トップに置かれるべきであり、取締役会は、サイバー・ヒューマン要因にどのように対処するかにおいて、積極的な役割を果たすべきです。

### 取締役会が自問すべき重要な質問

- 基本的なサイバーセキュリティ（ファイアウォール、ウイルス対策ソフトウェア、パッチ適用、パスワードの衛生など）は、どの程度堅牢で最新のものですか。
- 電子メールソフトウェアフィルタ、多要素認証、レポート作成手順、機密情報へのアクセス制御など、サイバー攻撃者の標的になることからスタッフを保護するために、どのようなセキュリティプロトコルを使用していますか？
- 従業員にどのようなサイバーセキュリティのトレーニングと情報を提供していますか？それは企業のすべてのレベルで行われており、関与を改善することができますか？
- 御社のサイバーセキュリティの責任者は誰ですか？全社的なアプローチを採用していますか。
- 社内ドメイン外からのメールはすべて「外部」と表示されていますか？直リンクはオフになっていますか？マクロは禁止されていますか？
- 有効な BYOD（Bring Your Own Device）ポリシーはありますか？これは、より多くのスタッフがリモートで作業する場合に特に重要です。
- BEC（Business E-mail Compromise）を防止するために、すべての電子送金に第二の手動認可／チェックが必要であることを確認していますか？

**取締役会がどのようにサイバーリスクを管理する必要があるかについての詳細は、**
Cyber Risk Oversight2020:Key Priorities and Practical Guidance for Corporate Boards from ISA
**（インターネット・セキュリティー・アライアンス）and ecoDa（ヨーロッパの主要な取締役協会を代表する組織）を参照。**

**www.aig.com**


**Mark Camillo**
Head of Cyber,
EMEA
T +44 (0)20 7651 6304
M: +44 (0)7860 261 692
mark.camillo@aig.com

**Sebastian Hess**
Cyber Risk Advisor,
EMEA
T +49 69 97113 572
M: +49 159 04611288
sebastian.hess@aig.com


AIG損保




AIG損害保険株式会社
〒105-8602 東京都港区虎ノ門 4-3-20

20-037005 (2020-09)