ivanti

2023
隠れた脅威

従業員の属性がセキュリティ体制に与える影響

Ivantiのサイバーセキュリティ現状レポートシリーズ

人口統計を深堀り

トップダウンの画一的な企業セキュリティでは、地域、年齢、性別、役割などに伴う固有のリスクが無視される傾向があります。

このIvantiの最新レポートでは、リスクの高い従業員の行動（最も注意意識の低い従業員は、あなたが思っているような人物ではない）から、セキュリティ文化の矛盾まで、あらゆることを調査し、全体像の平均を明らかにしています。

従業員の3人に1人は、自分の行動が企業のセキュリティに影響を与えることはないと考えている

Ivantiは、6,500人以上の経営幹部、サイバーセキュリティ担当者、一般の従業員（オフィスワーカー）を対象に調査を実施：

- サイバーセキュリティに対する従業員の意識と、防衛における従業員の役割認識
- セキュリティ担当者が診断する主な課題と脆弱性
- 経営幹部のテクノロジーとの付き合い方とサイバーセキュリティ戦略に対する賛同の度合い

目次:

01 **世代の神話:**
若いユーザーほどセキュリティに関して優れている」のか「?

02 **インシデントによる影響:**
年齢、性別、地域別のインシデント報告の傾向

03 **地域ごとの研修:**
研修やセキュリティ意識における地理的な違い

04 **解決するための行動:**
セキュリティ戦略におけるエンドユーザーの属性への対処法

ivanti

調査方法

Ivantiは、2022年第4四半期に 6,500人以上の経営幹部、サイバーセキュリティ担当者、一般従業員（オフィスワーカー）を対象に、今日のリスクを理解し、未知の将来の脅威に対して組織がどのように備えているかを明らかにするために調査を実施しました。

本レポートでは、組織のエンドユーザーの具体的な属性が、個人的な態度や行動にどのような影響を与えるか、また、これらの変動が脅威アクターに悪用される高度なリスクをどのようにもたらす可能性があるかに焦点を当てています。

調査対象

5,202人
一般従業員
40歳以下の回答者：3,609人
40歳以上の回答者：2,769人

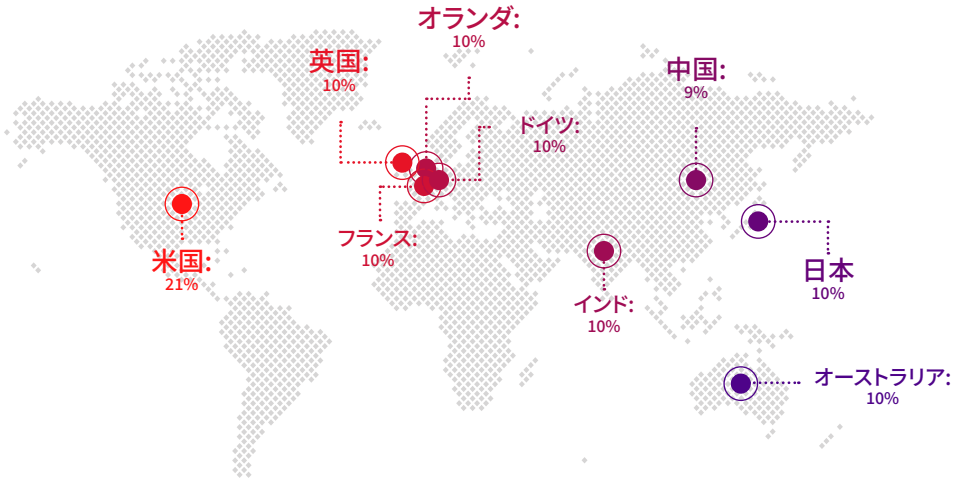
902人
セキュリティ担当者

454人
経営幹部

3,414人
女性

3,119 人
Male

27人
二者択一でない/答えたくない



01

世代の神話:

若いユーザーほどセキュリティに関して「優れている」のか?

ivanti

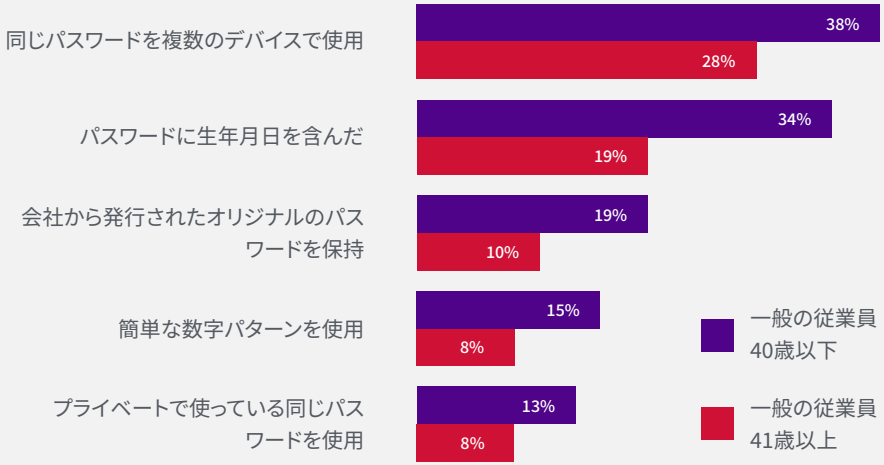
現在の問題

多くの人は、年齢が高い従業員は技術的な知識が乏しく、それゆえに危険な行動に走りやすいと考えています。実際はその逆です。

若い従業員（40歳未満）は、X世代以上の従業員と比較して、重要なセキュリティガイドラインを無視する傾向が顕著です。これは、パスワードの衛生管理、フィッシングリンクのクリック、家族や友人とのデバイスの共有についても言えることです。

若い従業員ほど、安全でないセキュリティ習慣を身につけている可能性が高いと言えます。

Q： 職場でログインパスワードの作成を求められたとき、過去2年以内にどのようなことをしましたか?



	一般の従業員 40歳以下	一般の従業員 41歳以上
標的にされ、フィッシングリンクをクリックした	13%	8%
家族や友人と仕事用のデバイスを共有した	34%	19%

重要な理由

このような過失、不注意、短絡的な行動が積み重なると、若い従業員のセキュリティ脆弱性は著しく高くなります。

年齢によるテクノロジーへの習熟度についての固定観念は、組織を迷わせるかもしれません。そしてこの問題は、サイバー衛生（パスワードの習慣、デバイスの共有など）だけに関連しているのではありません。調査によると、若手の従業員は、疑わしい問題に遭遇しても、それを報告する可能性が低くなっています。

40歳以下の労働者のうち、23%が最後に受け取ったフィッシングメールやメッセージを報告しなかったと答えています。

報告しなかった最も一般的な理由

「報告が重要だとは思っていなかった。」

フィッシングメッセージをセキュリティに報告しなかった従業員

技術職の従業員は、年齢層が低いため、年齢が高い従業員に対する固定観念は特に陰湿です。そのため、年齢が高い同僚は知識が不足していたり、脆弱であったりすると考える傾向が強いかもしれません。

たとえば、英国の2,250人の担当者を対象にした調査では、技術職の従業員が38歳になると、同僚を「年を取りすぎている」、「仕事をするには年を取りすぎている」と見なすことがわかりました。[1]

（これは、技術に疎い平均的な従業員ではなく、技術業界の同業者との比較であることに注意してください。）

これらの調査結果は、組織が従業員個人の判断に頼るのではなく、ルールに従うことを容易にする技術的介入に頼る必要がある理由を明確に示しています。

さらに良いのは、エンドユーザー（従業員）がその存在に気づかないような、完全にバックグラウンドで実行される自動化の導入を検討することです。

「若い従業員ほどセキュリティ意識が高く、テクノロジーに精通していると考えるのは時代遅れであり、危険でさえあります。組織は、従業員のセキュリティリスクに対する考え方や、従業員がセキュリティリスクを管理する役割を把握する内部調査を実施することによって、こうした思い込みを実証する必要があります。」

ダニエル・スパイサー（Daniel Spicer）
Ivanti、最高セキュリティ責任者

02

インシデントによる影響:

年齢、性別、地域別のインシデント報告の傾向

ivanti

現在の問題

組織を安全に保つということは、セキュリティインシデントや侵害に関する情報をほぼリアルタイムで入手することを意味します。当社の調査によると、危険な兆候を報告したがらない従業員もいます。

セキュリティ上の懸念がある場合、従業員はすぐに相談することができますか？　Ivantiの調査によると、従業員の特定の層は、自分から連絡を取ることをためらう可能性があります。これは、アウトリーチや研修プログラムを開発する際に、各団体が留意すべき点です。

年齢

報告で最も大きな変動要因は年齢です。当社が調査したリーダーの72%が、サイバーセキュリティ担当者に質問や懸念を問い合わせたことがあると回答しているのに対し、一般の従業員はわずか28%でした。

性別

女性は男性よりもその傾向が弱くなります。疑問や懸念をサイバーセキュリティ担当者に問い合わせたことがある人は 28%で、男性の36%を上回っています。

知っていましたか？

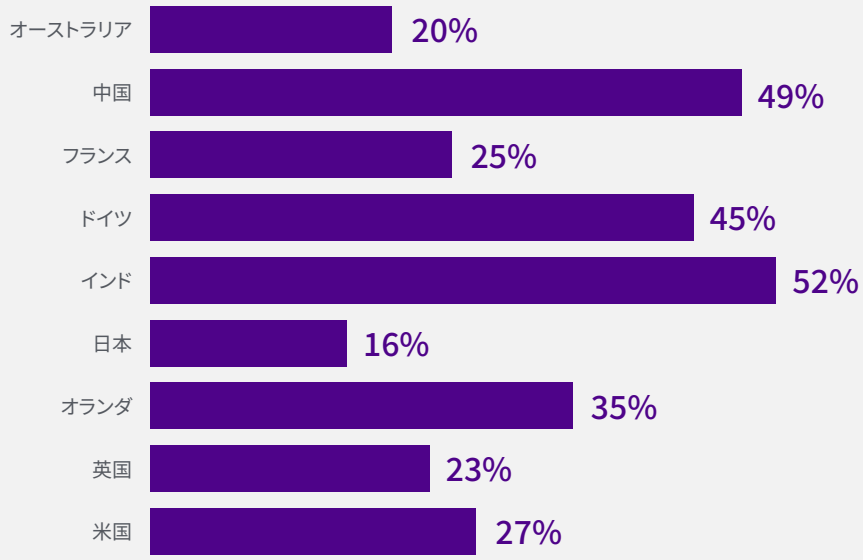
経営幹部は、セキュリティ上のやり取りを「気まずい」または「恥ずかしい」と思う傾向が、従業員よりも2倍高いのです。[2]

このような、より頻繁かつネガティブなセキュリティ上のやり取りは、経営幹部が社外の非承認テクノロジーを利用するのを加速させる可能性があります。

セキュリティに対するユーザーの意欲は国によって大きく異なっています。

たとえば、中国では一般従業員の半数近くが質問や懸念をセキュリティ部門に問い合わせたことがあるのに対し、オーストラリアではわずか20%にすぎません。

セキュリティに質問や懸念を伝えた従業員 (地域別)



重要な理由

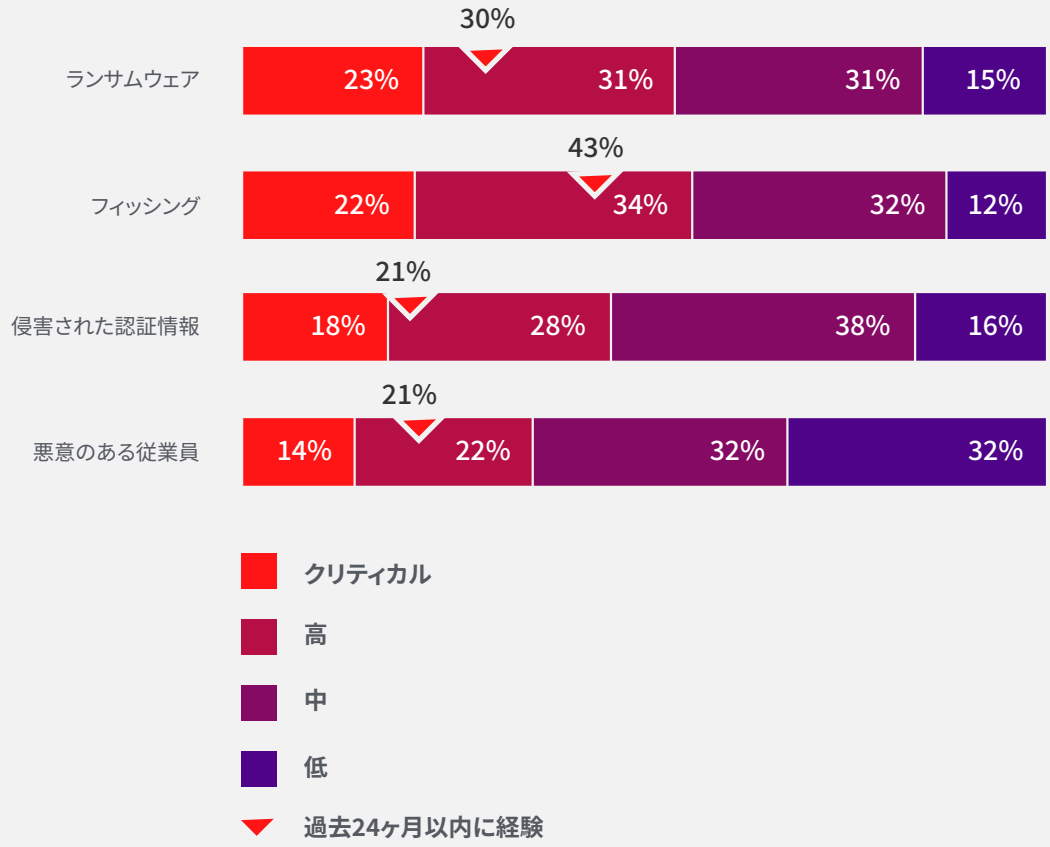
セキュリティの状況は、何千人もの従業員が防御をどう行うかにかかっています。その従業員は、自分たちがセキュリティチームの貴重なメンバーであることを理解しているでしょうか。

Ivantiの主要なセキュリティ対策調査は、セキュリティ担当者に業界全体の最大の脆弱性について質問したものです。ランサムウェアが1位、フィッシングが2位です。

そして、このような脅威は年を追うごとに危険性を増しています。特に、フィッシングの検出を難しくしている生成 AI の進歩がこれに寄与しています。

上位に挙げられたセキュリティ上の脅威と弱点は、従業員を守るための好機となります

Q: あなたの業界における 2023年の脅威のレベルを、次の項目ごとに評価してください。



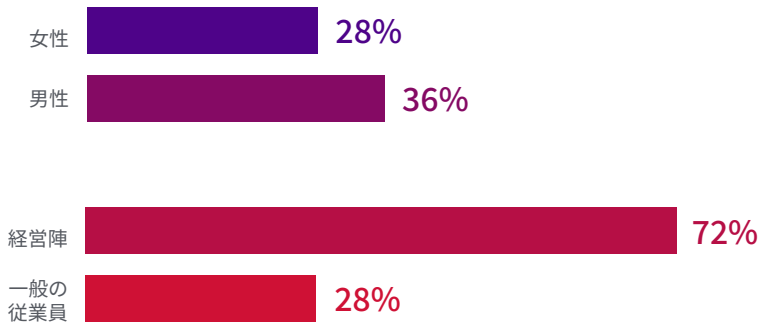
このような脅威の加速とリスクの増大は、従業員が気軽にセキュリティ部門に相談できる必要があることを意味します。たとえ、攻撃が迫っているという「証拠」がわずらわしい疑念だけであったとしてもです。

（例: 通常とは異なる電信送金依頼、不審な請求書の催促、または未承諾のパスワードリセットリンク）

つまるところ、アクティブなセキュリティインシデントが発生している間は、攻撃から身を守るために最も重要なのはスピードなのです。

最終的には、企業が従業員の態度を理解するためにセンチメント調査を実施する場合、人口統計学的なパターンと脆弱性を掘り下げて調査することが求められます。

セキュリティ担当者に質問や懸念を問い合わせたユーザー



「高度なフィッシング攻撃を何度か経験しましたが、従業員は標的にされていることに全く気づいていませんでした。この2年間でこの種の攻撃は非常に巧妙になり、経験豊富な者でさえこの攻撃に引っかかってしまうのです。」

— 2023　Press Reset　調査より[3]

03

地域ごとの研修:

研修やセキュリティ意識における地理的な違い

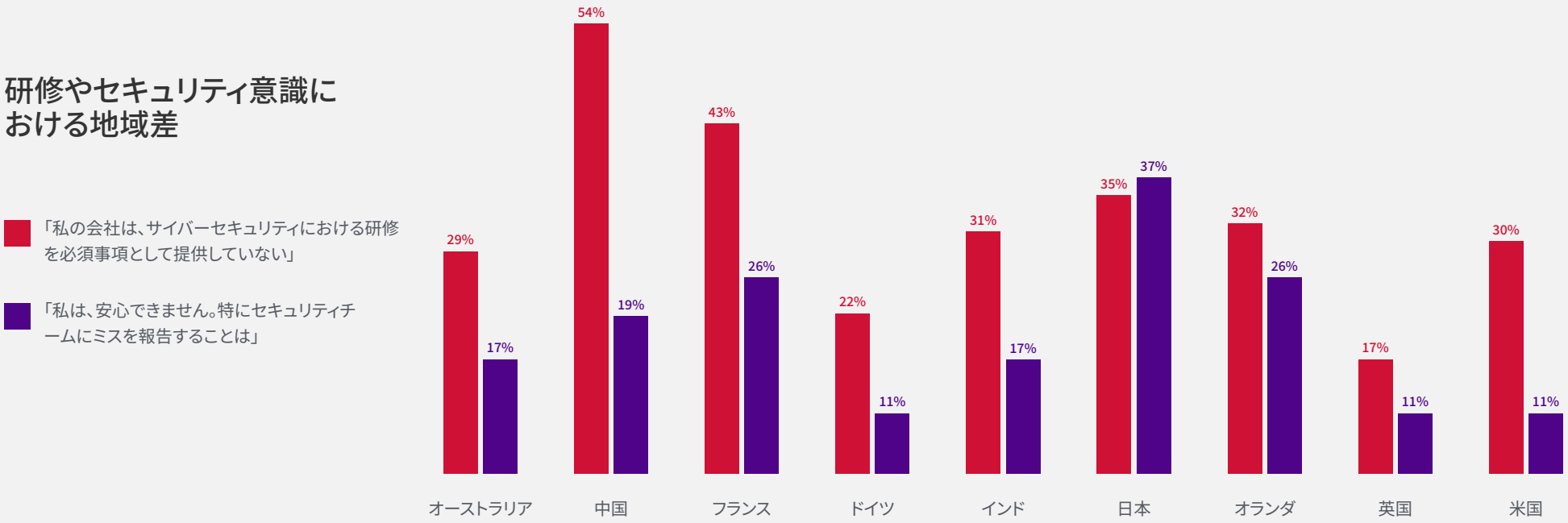
ivanti

現在の問題

組織の文化や研修プログラムは、セキュリティへの準備態勢に大きな影響を及ぼしますが、当社の調査によると、この2つは国によってばらつきがあります。

Ivantiの調査によると、国ごとのセキュリティ文化には、組織から提供される研修、リーダーや一般の従業員レベルの態度の両面で、重要な違いがあることがわかりました。

研修やセキュリティ意識における地域差



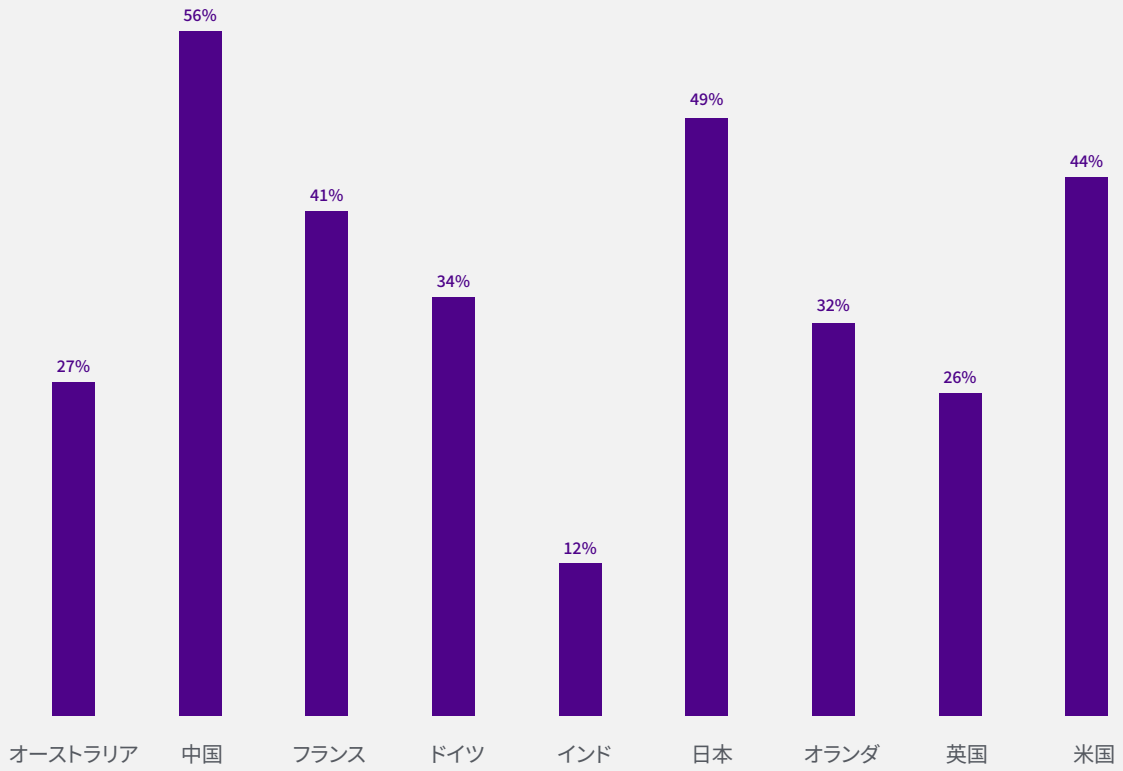
重要な理由

多くの組織は、研修やセキュリティ文化に対してトップダウンのアプローチをとっていますが、調査によると、首尾一貫した計画をまとめるには、地域のセキュリティ文化、さらには地域の文化を理解することが極めて重要であることがわかります。

どこの出身であろうと、新入社員は皆、意図的であろうとなかろうと、組織に独自の脆弱性を持ち込んでいるものです。研修が十分でない従業員は、組織全体の備えの強さを薄めてしまう危険性があります。

このリスクを最小化するために、企業はグローバルおよび地域レベルで、強力なオンボーディングと継続的なセキュリティ研修プログラムに投資する必要があります。

オフィスワーカー（従業員）「自身の行動は、組織が（サイバー脅威から）安全を保つ能力に影響を与えません。



地域文化とグローバルセキュリティプログラムとの関係

文化は、組織がどのように資産や人を守るか、また攻撃に対してどのように対応するかに影響を与える可能性があります。

カルチャーによって考えられるセキュリティへの課題

グローバルレベルのトレーニングに対する**従業員の不快感**（例：教材を現地の言語や文化にうまく翻訳できない

地域レベルで「社会化」されていない**新しい基準や規則に対する従業員の不安**

個人の失敗や懸念を報告する余地をほとんど与えない、**トップダウンの現地オフィス文化**

例えば、従業員が質問や懸念を抱いた場合、**別の国のセキュ リティチームメンバー**に連絡を取らなければならず、言語や文化的な障壁

このような国毎の違いは、準備体制を把握する上で興味深い指標となる

セキュリティチームが、最大規模のオフィスや最寄りのオフィスで起きていることを基準にセキュリティを判断するのは簡単で、よくあることだ

この調査は、本社、研究開発施設、サプライチェーン拠点、製造拠点など、あらゆる場所でより詳細なデータを調査し、セキュリティ手順を明らかにすることがいかに重要かを示している。

ダレン・ゴーソン（Daren Goeson）
Ivanti、製品管理担当上級副社長

04

解決するための行動:

セキュリティ戦略における エンドユーザーの属性への対処法

ivanti

解決するための行動

大局的な卓越性には、リスクが隠されていることがあります。

ここでは、人口統計に関連するセキュリティリスクについて詳しく説明します。特定の組織における人口統計リスクをどのように評価するか、また、適切な対策を講じるためにどのようにアプローチを調整するかについて掘り下げます。

隠れたリスクを是正する5つの方法

1. **従業員を調査します。**
   ユーザーのセキュリティ意識と行動が、これらのグローバルベンチマークと比較してどのような状況に置かれているかを確認します。
2. **固定観念にとらわれないようにします。**
   セキュリティチーム自身が持っている可能性のある仮定やバイアスを調べます。
3. **資料をローカライズします。**
   基本的な翻訳にとどまらず、トレーニングや方針が地域の誤解を招かないようにします。
4. **バックエンドを再設計します。**
   可能なかぎり従業員の関与を排除し、自動コンプライアンスを強化します。
5. **文化を再構築します。**
   セキュリティチームの対応に対する従業員の信頼と信用を高め、組織全体のセキュリティを向上させます。

隠れたリスクの是正 1:

従業員にアンケートを実施し、組織独自の人口統計学的習慣を明らかにします。

匿名アンケートを利用して、潜在的な人口統計学的差異に注意を払いながら、従業員層に関する洞察を明らかにします。(予想外の結果がありましたか。当初の想定を覆す回答パターンはありましたか。)

研修やアウトリーチ活動を強化し、さらなる支援を必要とする従業員層に合ったソリューションを提供するために、調査結果を活用します。

従業員の態度に関する匿名調査の質問例

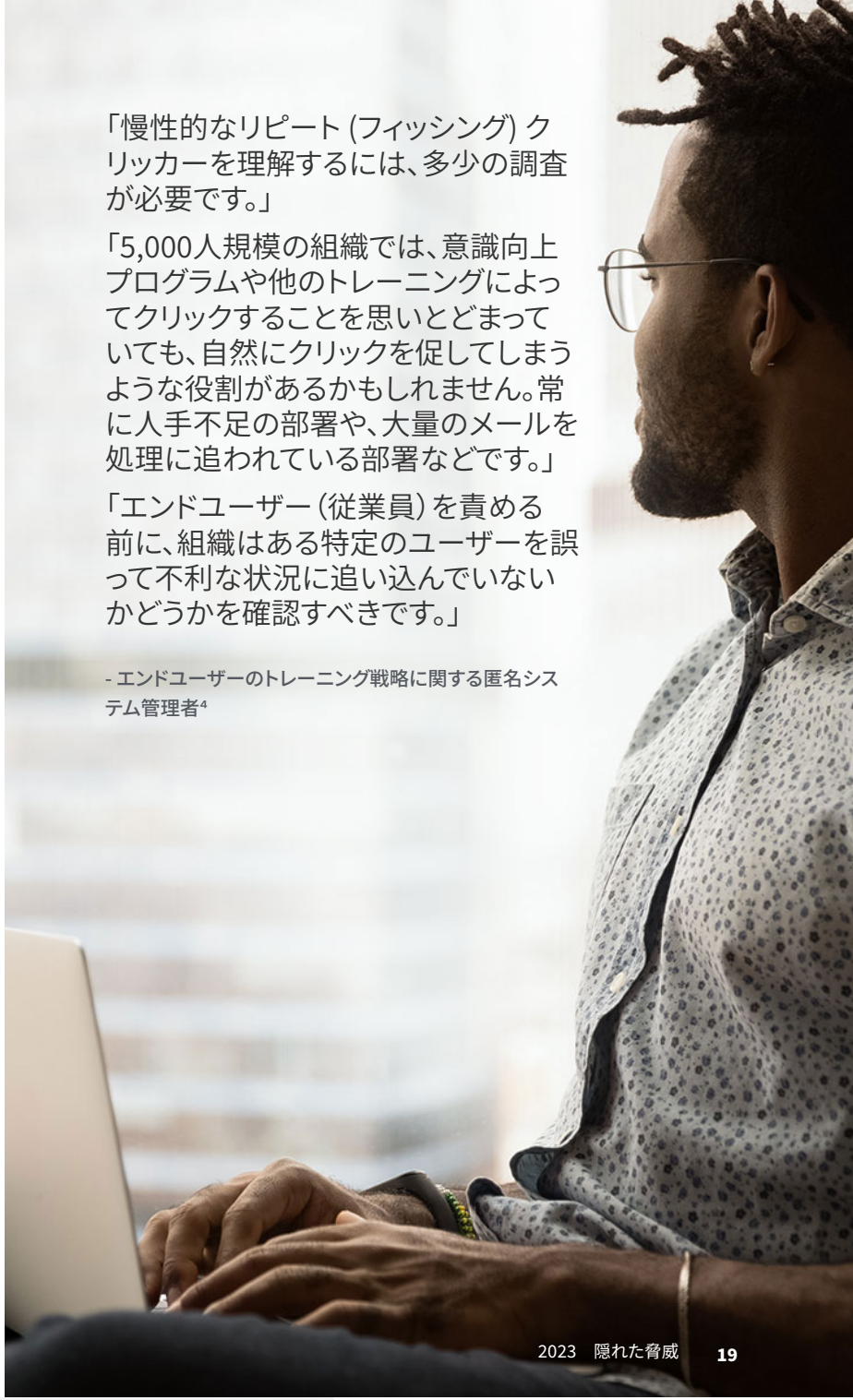
フィッシングを見分けられますか?

フィッシングを特定するための情報源やツールは与えられていますか?

セキュリティーチームに気軽に質問できますか?

セキュリティーチームにエラーを報告しても気持ち的に大丈夫ですか?

自身の行動が組織のセキュリティに影響を与えていると思いますか?



「慢性的なリピート (フィッシング) クリッカーを理解するには、多少の調査が必要です。」

「5,000人規模の組織では、意識向上プログラムや他のトレーニングによってクリックすることを思いとどまっていても、自然にクリックを促してしまうような役割があるかもしれません。常に人手不足の部署や、大量のメールを処理に追われている部署などです。」

「エンドユーザー (従業員) を責める前に、組織はある特定のユーザーを誤って不利な状況に追い込んでいないかどうかを確認すべきです。」

- エンドユーザーのトレーニング戦略に関する匿名システム管理者[4]

隠れたリスクの是正 2:

ユーザーのデジタル慣れと安全性に関する固定観念を取り払います。

セキュリティチームに、さまざまな従業員グループに関する思い込みを調べる匿名アンケートに答えてもらいます。そして、その結果を一般的な従業員調査の結果と比較することで、不当であるばかりでなく真実ではない思い込みを明らかにし、そのような固定観念がセキュリティ態勢にどのような影響を及ぼす可能性があるのかを明らかにします。

セキュリティ担当者に影響する3つの「ヒト」ベースの脆弱性

満足

最良の結果を得るために全力を尽くすのではなく、最低限実現可能な結果を得るために努力する具体的な意思決定プロセス。[5]

このプロセスを通じて焦点を絞ることは、リソースに乏しいチームの助けになるが、チームが基本的な実施には「十分重要でない」として放棄すると決定したものは、他の視点が考慮されることで、影響を受けたり、完全に変化したりする可能性がある。

無視の確率

ある出来事が大きな影響を及ぼすとき、人はその可能性を考慮しないことが多い。

調査によると、セキュリティ担当者は、たとえエンドユーザがセキュリティインシデントの可能性を報告しないといった小さなリスクの方が統計的に可能性が高いとしても、可能性は低いが被害が大きい事象を優先して是正したくなることが多いという。[6]

自信過剰バイアス

高度なトレーニングを受けた人は、自分の能力を過大評価する傾向があり、専門家のリファレンスと自分の解決策を照合したり、同僚からフィードバックを求めたりすることを省略してしまう。

セキュリティの担当者を対象としたある調査によると、セキュリティの担当者が一般的な教育やトレーニングを受けていると報告すればするほど、様々な意思決定バイアスに陥りやすいことがわかった。[7]

隠れたリスクの是正 3:

グローバルなセキュリティ文化がどのように翻訳され、ローカライズされているかを理解します。

セキュリティ研修やポリシーのような部門横断的なプログラムについては、資料を正しい言語に翻訳するだけでは十分ではありません。セキュリティ資料を「ローカライズ」し、その核となる意味が、文化的に混乱しやすいハードルを乗り越えるようにしなければなりません。

そのため、翻訳に先立ち、現地チームや地域チームに積極的に相談し、新しい資料に対する意見や賛同を求めます。

そして忘れてはならないのは、地域のリーダーは強力な伝達者になり得るということです。彼らは、他の地域の従業員が自然に理解し、信頼し、従うような方法で、あなたのセキュリティメッセージを自然に共有することができます。

セキュリティプログラムやコミュニケーションのためのローカリゼーション ライゼーションチェック

色

中国のユーザーは、赤のフラグがついたアイテムを幸運でポジティブなものとして見るかもしれない。インドネシアや南米のユーザーは、緑色はそれぞれ不倫や死を連想し、否定的な反応を引き起こすかもしれない。[8]

スポーツ

英語-アラビア語／アラビア語-英語の教材を対象としたとある研究では、基本的な翻訳では、スポーツ慣用句の「不適切な」訳語置換が37%の割合で見られた。9　スポーツ慣用句の翻訳に関する他の研究でも、ポーランド語10、ペルシア語／ペルシャ語11、その他ほとんどすべての言語で同様の困難が見つかっている。

シンボル

多くの英語圏では、チェックマークは「正解」または「完答」を象徴する。逆に、スウェーデンや日本では、チェックマークは不正解を示し、「R」や「O」は正解を示す。12　絵文字の意味さえも、ユーザーの世代13や地域14によって変わる！

隠れたリスクの解決 4:

技術スタックを設計して、ユーザーの不適合や不整合のポケットを最小限に抑えます。

個々のユーザーがセキュリティプロトコルに準拠することに依存するのではなく、エンドユーザーから効果的に隠蔽された、コンプライアンスを摩擦のないものにするための介入として、より強力なバックエンドの自動化を構築します。

エンドユーザーの摩擦を減らす3つの一般的なセキュリティアップグレード

ジャストインタイムのセキュリティアップデート

ほとんどの従業員は、アップデートのためにコンピュータをシャットダウンして再起動することを好まない。そのため、このプロセスをいつまでも先延ばしにしてしまうか、あるいは単に再起動するのをすっかり忘れてしまいがち!

その代わりに、所定の時間内に自動的に再起動させるが、ユーザーが勤務時間外に再起動をスケジュールできるシステムを使用し、タイムリーで便利なアップデートを促す。

モダンなパスワードポリシー

最近、多くのグローバルなサイバーセキュリティフレームワークは、ユーザーの秘密が暴露された証拠がない場合、パスワードをローテーションする旧来の推奨を静かに廃止した。[15] - 新しいパスフレーズやPINを考え出す(そして覚える)のに苦労するから。[16]

その代わりに、パスワードマネージャー、シングルサインオンポリシー、またはパスワードレステクノロジーの導入を検討する。

サイレント利用ポリシー(AUP) - エンフォースメント機能搭載

従業員の入社時に、組織のAUPを確認することがあるかもしれませんが、実施されないポリシーは、印刷された紙の価値がありません。

特定のユーザープロファイルとアクセス権限に合わせてデジタルインフラ全体を構成します。基本的なアクセス権限が各自の作業負荷に対して不十分な場合、ユーザーが高度なアクセス権限を要求する簡単な方法を備えています。[3]

隠れたリスクの解決 5:

オープンで歓迎されるセキュリティ文化を積極的に構築します。

この隠れた脅威レポートの調査結果は、すべての組織における協調的かつ積極的なセキュリティ文化の必要性を強調しています。つまるところ、従業員はセキュリティの担当者に連絡することを躊躇してはいけ ません。どれほど些細な質問であっても、また愚かな過ちの可能性があったとしてもです。

非懲罰的なセキュリティ文化においてのみ、セキュリティチームは、組織全体を適切に保護するために、ユーザーから十分な協力を得ることができるのです。

強固なセキュリティ文化の4つの重要な考え方

オープン

従業員は安心してインシデントを報告し、その正直さと透明性が評価されるべきです。従業員は、どんなに些細な質問であっても、安心してセキュリティ・チームに近づくことができます。

反復的

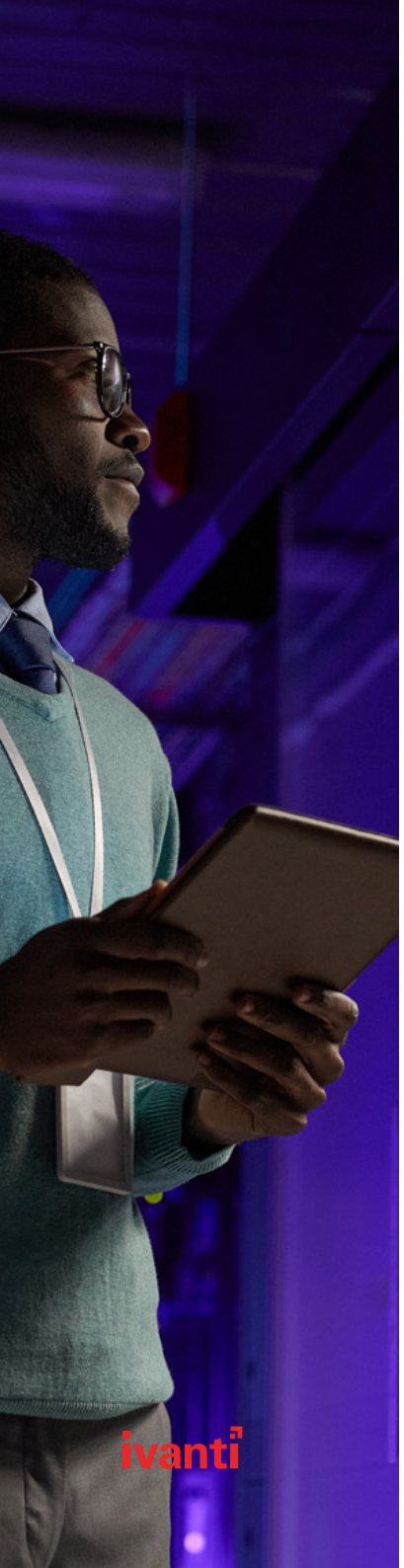
この組織では、正式なトレーニングワークショップや組織全体への定期的なコミュニケーションから、実際のセキュリティシナリオを題材にしたゲーム化されたセキュリティコンテストまで、従業員にとって説得力のあるトレーニングを頻繁に繰り返し実施しています。

デザイン

従業員の行動は、テクノロジー主導の行動介入によって研ぎ澄まされます。これらのテクノロジーは、シャドーITの回避策や一般的なコンプライアンス違反を大幅に削減するよう、うまく設計されるべきです。

統合

組織のセキュリティに対する責任は全員が共有するものであり、従業員は組織の安全を守ることに投資されています。



参考文献

1. Sevilla, C. (2022, May 23). Everyday ageism in the tech industry. From CWJobs: https://www.cwjobs.co.uk/advice/ageism-in-tech
2. Ivanti. (2023, August 29). 2023 Executive Security Spotlight: New research from Ivanti shows real risks facing the C-suite. From Ivanti: https://www.ivanti.com/resources/v/doc/ivi/2773/17cca519291d
3. Ivanti. (2023, December 12). Press Reset: A 2023 Cybersecurity Status Report. From Ivanti: https://www.ivanti.com/resources/v/doc/ivi/2732/7b4205775465
4. u/CyberAndFolkloreGuy. (2023, January 19). Security Awareness: How to properly address colleagues who repeated fail Phishing tests? From Reddit: https://www.reddit.com/r/cybersecurity/comments/10g4688/comment/j55k4cn/
5. Frankenfield, J. (2022, August 23). Satisficing: Definition, How the Strategy Works, and an Example. From Investopedia: https://www.investopedia.com/terms/s/satisficing.asp
6. De Wit, J. J., Pieters, W., & Van Gelder, P. H. (2022). Individual Preferences In Security Risk Decision Making: An Exploratory Study Under Security Professionals. WIT Transactions on The Built Environment, 187-199. doi:10.2495/SAFE210161
7. De Wit, J., Pieters, W., Jansen, S., & van Gelder, P. (2021). Biases in Security Risk Management: Do Security Professionals Follow Prospect Theory in Their Decisions? Journal of Integrated Security and Safety Science, 1(1), 34-57. doi:https://doi.org/10.18757/jisss.2021.1.5700
8. Eriksen Translations. (2020, February 3). How Translating Colors Across Cultures Can Help You Make a Positive Impact. From Erksen Translations: https://eriksen.com/marketing/color_culture/
9. Nasser, L., & Al-Aazzawi, K. (2022). Context Impact in Translating Sport Idiomatic Expressions from English into Arabic with Regard to Types of Idioms. Adab Al-Rafidayn Journal, 1-26. doi:10.33899/radab.2021.170415
10. Mazurkiewicz, M. (2014). Sports Vocabulary and Idioms – Some Observations About the Specificty of English-Polish and Polish-English Translation. Cultures and Literatures in Translation, 140-153. From https://www.academia.edu/40425597/Sports_Vocabulary_and_Idioms_Some_Observations_about_the_Specificity_of_English_Polish_and_Polish_English_Translation
11. Suzani, S. M. (2007). Sports Idioms and Duality of Meaning in Translation. Iranian Journal of Translation Studies. From https://journal.translationstudies.ir/ts/article/view/126

12. Grove, L. (1989). Signs of the times: graphics for international audiences. International Professional Communication Conference 'Communicating to the World', 137-141. doi:10.1109/IPCC.1989.102119

13. Brants, W., Sharif, B., & Serebrenik, A. (2019). Assessing the Meaning of Emojis for Emotional Awareness - A Pilot Study. Companion Proceedings of The 2019 World Wide Web Conference, 419–423. doi:https://dl.acm.org/doi/abs/10.1145/3308560.3316550

14. Gao, B., & VanderLaan, D. P. (2020). Cultural Influences on Perceptions of Emotions Depicted in Emojis. Cyberpsychology, Behavior, and Social Networking, 567-570. doi:https://doi.org/10.1089/cyber.2020.0024

15. National Institute of Standards and Technology (NIST). (2020, March 03). NIST Special Publication 800-63B. From https://pages.nist.gov/800-63-3/sp800-63b.html#sec5

16. WIlson, K. R.-H. (2020, March 9). The Debate Around Password Rotation Policies. From SANS Institute: https://www.sans.org/blog/the-debate-around-password-rotation-policies/

17. u/securebxdesign. (2023, April). What does your policy/training look like for people who fail phishing campaigns? From Reddit: https://www.reddit.com/r/cybersecurity/comments/13csxs0/comment/jjk37bo/

2023　隠れた脅威

従業員の属性がセキュリティ体制に与える影響

Ivantiのサイバーセキュリティ現状
レポートシリーズ

ivanti

ivanti.com/ja/
03-6432-4180
contact@ivanti.co.jp