ivanti

政府系サイバーセキュリティ現状レポート

2023年に取り組むべき行動と変化の推進の指針となる 4 つの重要なポイント

Ivanti のサイバーセキュリティ現状レポート シリーズの一部

タイミングは今です

昨今、病院ネットワーク、グローバルな物流システム、さらには民主的な選挙に対する攻撃があり、公共の安全とガバナンスに対する根本的な脅威となっています。

しかし、これはまだ序の口です。

Generative AI（生成AI）と「ディープフェイク」の急速な進化により、ランサムウェアはさらに巧妙化し、より危険なものになろうとしています。

世界中の政府も注目しています。バイデン大統領からの新たな指令や欧州委員会からの指令により、重要な資産やインフラをサイバー攻撃から保護することが世界的に急務となっています。

Ivantiは、全世界の 800 人以上の政府職員を対象に調査を実施し、次の点を把握しました。

- サイバーセキュリティに対する従業員の行動と意識
- 公共部門における柔軟なハイブリッドワーク環境の影響
- サイバーセキュリティの専門家から見た新しい脅威とセキュリティテクノロジー

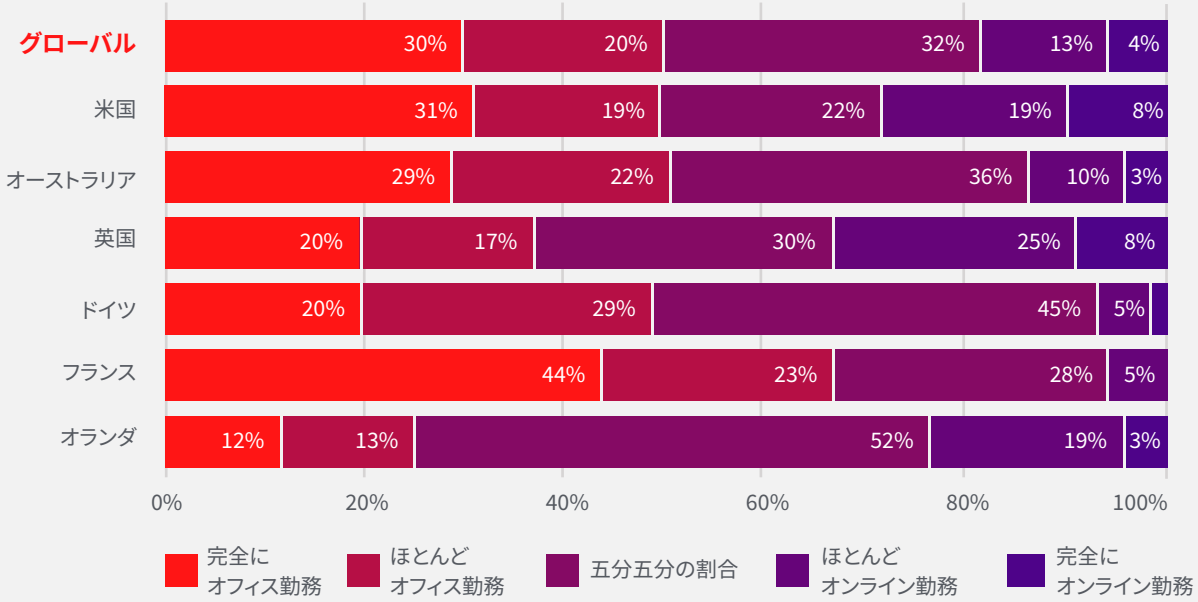
なぜ全力で緊急性をもって取り組むべきなのでしょうか。

新しい攻撃モードや注目される政府の指令だけではありません。わずか数年で、政府機関の業務の本質が大きく変わりました。このような劇的な変化の前に、一般的に行われるような事前の計画はまったくありません。ハイブリッドワーク環境によって、脆弱性の新しい領域が生じました。

新しい現実

政府職員の 70% が、少なくとも一部の時間帯でオンライン勤務している

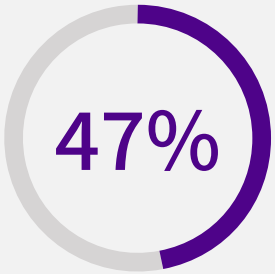
Q: あなたの組織でデスクワークをしている人の働き方について、最も当てはまる回答はどれですか。



*国別の結果は、四捨五入の誤差により100%にならない場合があります。

新しいリスク

働く場所の柔軟性、デバイス、ユーザーの急増が複雑さを増し、新たな脆弱性を生む



世界中のセキュリティ専門家が、ネットワーク上のすべてのユーザー、デバイス、アプリケーション、サービスに対して高い可視性がないと回答しています。

調査対象の政府職員が、複数のデバイスで同じまたは類似のパスワードを使用しています。

目次:

01 説明責任という文化がない

02 パスワードの（誤った）管理:
セキュリティの「ゼロ地点」

03 全員を対象としたトレーニング:
政府におけるサイバーセキュリティの人為的なギャップ

04 将来を見据えた政府機関

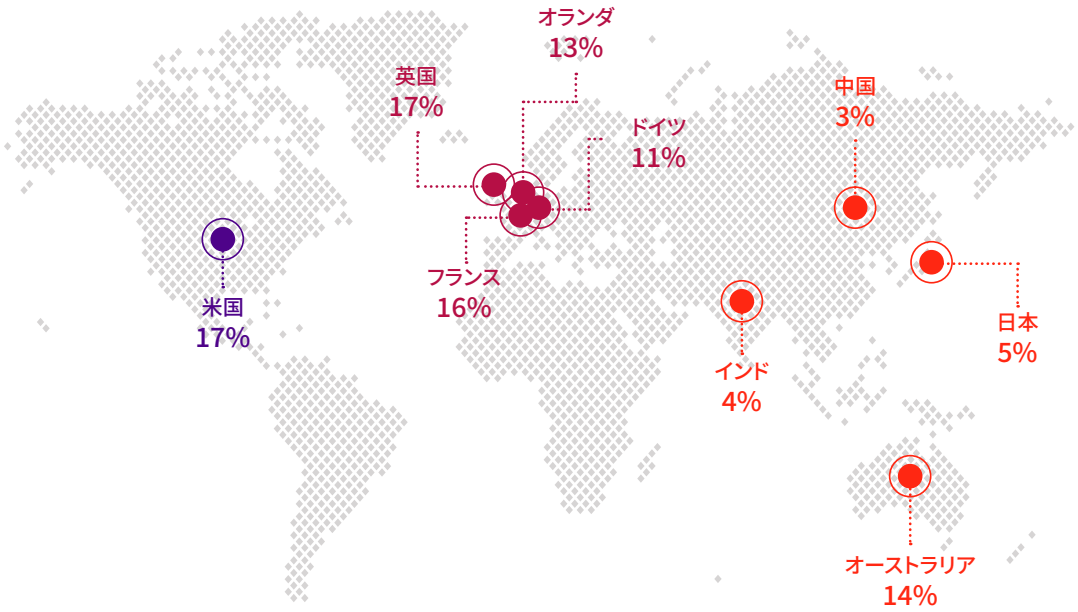
ivanti

調査方法

Ivantiは、2022年第 4 四半期に 6,500 人以上の経営陣、サイバーセキュリティ担当者、一般の従業員を対象に、今日の脅威を理解し、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。このデータは、Press Reset: 2023年サイバーセキュリティ体制の現状レポート で発表されています。

この調査で集められた見識は、この調査のサブセットである、世界中の政府機関で働く職員（合計 803 名）、および複数の業界のサイバーセキュリティ担当者の回答に基づいて考察されています。

調査対象の政府職員（n=803）



01

「説明責任という文化」がない

ivanti

現在の問題

「私の仕事ではない」という態度が、政府のサイバーセキュリティを危険にさらしている

従業員の無関心は、組織にとって現実のセキュリティリスクです。Partnership for Public Serviceによると、公共部門のエンゲージメントと満足度のスコアは、民間部門の従業員に比べ 15 ポイントも遅れをとっています。[1]

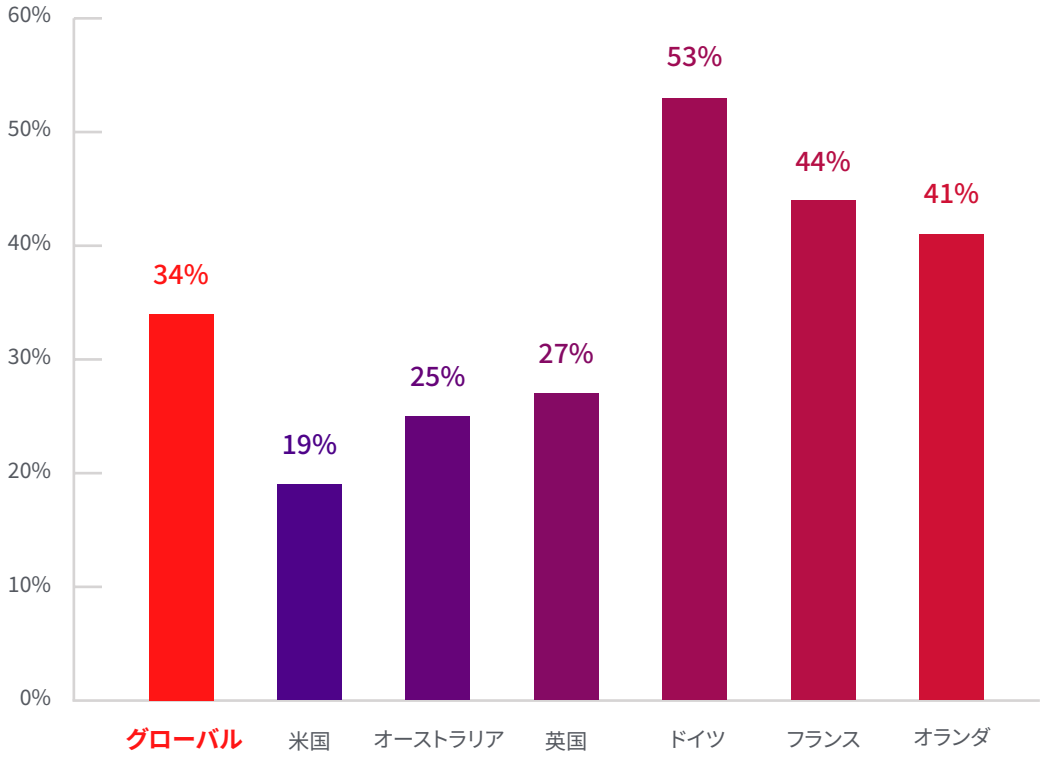
また、エンゲージメントが低いということは、従業員が組織全体とのつながりや説明責任を感じていないことを意味します。

Ivanti の調査データがこれを裏付けています。世界中の政府職員の多くが、セキュリティに関して自分の行動は重要でないと考えています。

英国では、27% の政府職員が、自分の行動がサイバー攻撃から組織を守ることに影響しないと回答しており、ドイツではその比率が 53%に上ります。

職員は自分の行動を重要視しているのでしょうか？

Q: 自身の行動がサイバー攻撃から組織を守ることに影響すると考えていますか。



「私の行動はサイバー攻撃から組織を守ることに影響しません。」

すべての政府職員が不審なアクティビティを報告するわけではない。

17% 業務上のセキュリティの過失をサイバーセキュリティチームに安心して報告できない。

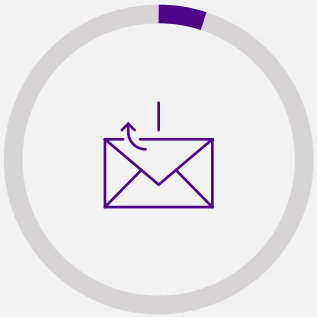
36% 業務中に受信したフィッシングメールを報告しなかった。

21% 組織がハッキングされても気にしないと回答している。

政府職員がフィッシング攻撃の対象になる - サイバー攻撃の序章

30%

フィッシング攻撃の対象になったと回答している。



5%

リンクをクリックしたり、送金してしまったりして、フィッシング攻撃の被害に遭った。

重要な理由

サイバーセキュリティの最悪の状況がすべての政府機関に迫る

複数の効果的な脅威ベクトル

公共部門は、ターゲットの規模や価値が大きいため、特に攻撃を受けやすくなっています。昨年、APT29 のような国家が支援する持続的脅威のハッカーは、いずれも手ごわく、急速に進化している敵であることが証明されました。[2]

急速に進化する「合成」デジタルコンテンツ

生成系 AI により、フィッシングメールが個々のターゲットの脆弱性に合わせてパーソナライズされ、フィッシングメールが「完璧な理想」になりました。[3]

さらに憂慮すべき点は、ディープフェイクが、世界中のジャーナリズムと民主的な選挙の信頼性を脅かすということです。[4]

予算の制約と組織のサイロ化により、セキュリティへの取り組みが弱まる

米国会計検査院（GAO）は、過去 10 年間にサイバーセキュリティに関する勧告の 60% が実施されていないと述べています。[5]

無関心な職員の割合が深刻化

米国連邦政府職員の平均エンゲージメントは 100 点満点中 64.5 点で、民間企業に 14 点もの差をつけられています。[6]

72%

政府職員がセキュリティ担当部署に質問したり、懸念を表明したりするために連絡したことがありません。

ivanti

行動に移す

セキュリティは全職員の間の共有責任とする

セキュリティのリーダーは、サイバーセキュリティに関心を持つように職員に強制することはできませんが、前向きなセキュリティ文化に投資し、その文化を醸成することで、長期的に従業員の態度に影響を与えることができます。

好ましいセキュリティ文化の要素

オープンである

職員が安心してセキュリティチームに質問できる

統合されている

セキュリティの説明責任を共有し、職員一人ひとりが役割を果たす

安全である

職員が安心してインシデントやミスを報告できる

反復的である

トレーニングが頻繁に行われ、繰り返され、説得力がある

戦略的である

セキュリティは組織の成功にとって非常に重要な資産である

次のステップ

好ましいセキュリティ文化のために、職員の経験を監査し、関与し、最適化する

1

監査

職員にアンケートを実施し、ベースラインを定義し、現在の行動や態度を記録します。この調査結果は、組織の具体的な弱点を特定し、変革のための実践的なロードマップを策定するために必要な情報源となります。

2

関与

組織のリーダーと関係し、サポートと同意を得ます。リーダーは、方向性を決定するだけではなく、最大のリスク領域の 1 つでもあります。

リーダーのサイバーセキュリティに対するリスクについては、19 ページ「政府組織機関を対象としたホエールフィッシング 101」）をご覧ください。

3

最適化

文化の変革は、決して「1 回で終わる」ものではありません。主要な業績評価指標を監視し、従業員の声に耳を傾け、必要に応じて軌道修正を行う必要がある、継続的なプロセスです。

02

パスワードの（誤った）管理:
セキュリティの「ゼロ地点」

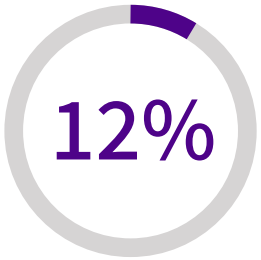
ivanti

現在の問題

悪いパスワードの習慣を含むサイバー衛生の不備が政府機関を悩ませている

セキュリティ担当者は、10年以上前からパスワードのリスクについて警鐘を鳴らしてきましたが、政府機関を含むほとんどの組織では、いまだにパスワード管理に対して緩いアプローチを取っている場合があります。Ivanti の調査では、政府の回答者からさまざまな悪い習慣が明らかにされました。

政府のパスワードアクセス不正行為

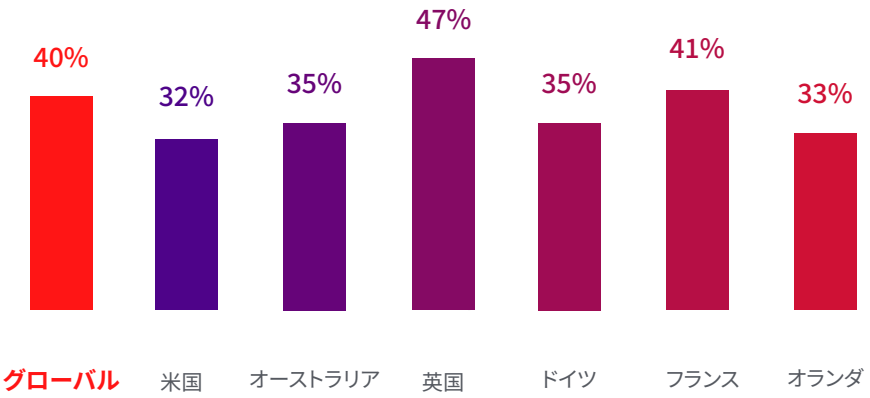


政府職員が、職務上必要のない機密情報にアクセスしたことを認めています。

3 人に 1 人

前職のパスワードがまだ使えると考えていると回答しています。

同じ業務用パスワードを 1 年以上使用している政府職員の割合



重要な理由

セキュリティと利便性の押し問答

いわゆる「シャドー IT」などの回避策は、安全な組織の敵です。従業員は、セキュリティ対策が非効率的であったり、負担が大きいと感じると、明らかに安全ではない回避策を見つけるものです。

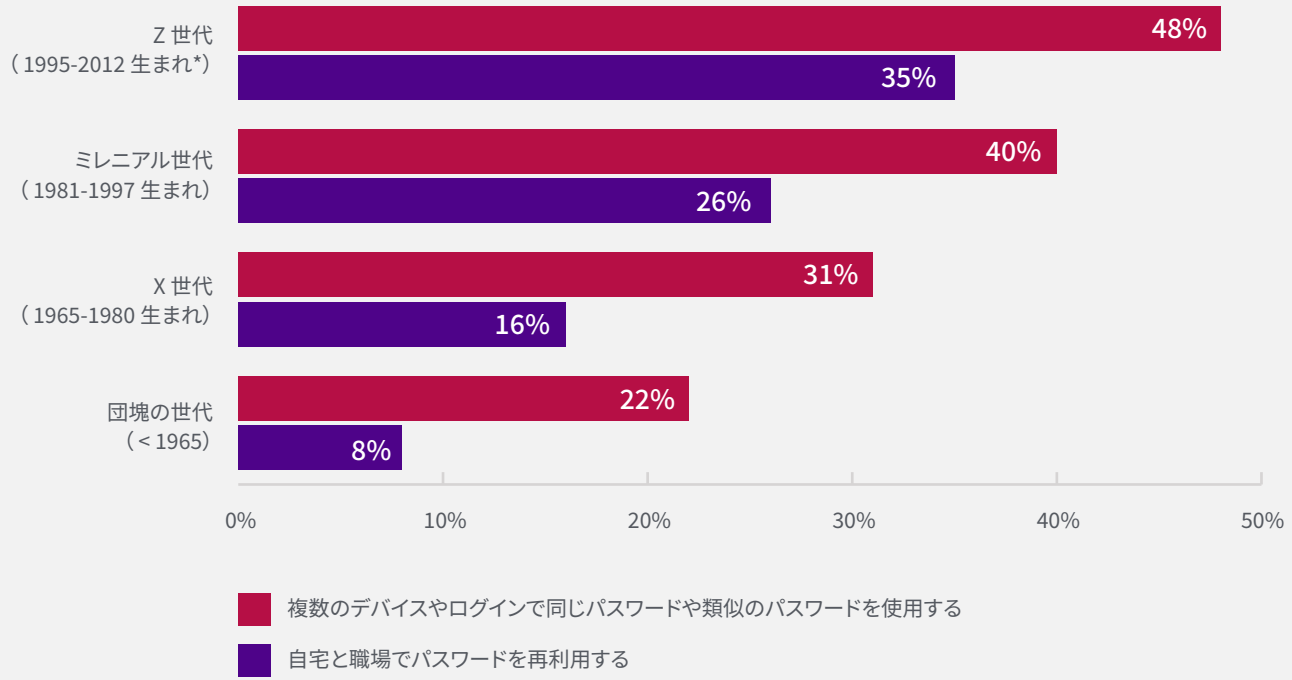
パスワードは、従業員のセキュリティ対策のゼロ地点です。あらゆる業界の従業員が、付箋、ペットの名前、誕生日、そして誰もが好きな解読不可能なコード「12345」を使い続けています。

政府機関は、職員がいわゆるソリューションを回避する方法を探さないような、便利で簡単なセキュリティソリューションを必要としています。

「デジタルネイティブ」の神話

若手従業員はパスワードのセキュリティに精通していると思いますか。
データによる裏付けはありません。

Q: 職場でログインパスワードの作成を求められたとき、この 2 年間で次のうちのどれをしたことがありますか。



*18 歳以上の回答者のみ。

解決するための行動

デジタル従業員体験 (DEX) に投資し、セキュリティを高める

セキュリティチームは、デジタル従業員体験 (DEX) というレンズを通して新しいポリシーやテクノロジーを評価し、「エンドユーザー体験は、利便性のために回避策やその他の好ましくない行動を促すだろうか、もしそうなら、そのリスクはそれに見合うものだろうか」と自問するべきです。

次のステップ

セキュリティを確保しながら、使いやすい体験を実現

1

危険度の高い回避策に的を絞る

- 従業員は利便性の名の下にセキュリティを回避する
- 上級幹部がセキュリティ規則の適用除外を要請する

2

DEX に特化したテクノロジーを優先

- ユーザー中心の体験を実現する (摩擦が少ない＝コンプライアンスが高い)
- 可能な限り、人の手を介さない
- 免除のロックダウン

実世界への影響

ゼロトラストアーキテクチャ（ZTA）の実装とDEXの考慮点

二要素認証、トークン、生体認証データのいずれを使用するにしても、組織や機関は、ゼロトラストアーキテクチャ（ZTA）戦略に従って、すべての従業員に対して最小特権アクセスモデルを優先させ、それを約束する必要があります。

ZTAでは、セキュリティとITソリューションが連携し、従業員に対して必要な範囲のアクセス権のみを提供することで、セキュリティ態勢とコンプライアンスを継続的に検証します。

この限定されたアクセスは、セキュリティ上の利点のほか、組織のセキュリティを確保しつつ、柔軟な勤務形態を可能にします。

結局のところ、従業員がフィッシング攻撃に屈した場合でも、脅威主体は従業員が利用できる限られた選択肢にしかアクセスできません。

しかし、ZTAでは日々の運用（従業員）や保守（IT担当者）が過度に煩雑になり、シャドーITの利用を促し、ZTAの利点を損ねてしまう可能性があります。

このため、ZTAを検討している組織は次の方法を活用してください。

- 不明なデバイスの通知、疑わしい行動のアラート、ユーザー権限のアクセスタイムアウトを戦略的に自動化する。
- アクセス許可要求や一般的な問い合わせのためのITプレイブックと意思決定ツリー。
- エンドユーザーがITチケットを送信する前に、直感的で簡単にアクセスできる「セルフサポート」手順。

ZTAとDEXに関するその他のリソース

- NIST Special Publication 800-207（「ゼロトラストアーキテクチャ」）
- NISTサイバーセキュリティのフレームワーク（CSF）：IvantiのソリューションのCSF統制へのマッピング
- 2022年版レポート：従業員のデジタル体験を向上させる必要性
- DEX（従業員のデジタル体験）から始めましょう
- Everywhere Workplaceの従業員体験ITが企業をリードすべき理由

03

全員を対象としたトレーニング: 政府の人間規模のサイバーセキュリティギャップ

ivanti

現在の問題

サイバーセキュリティのトレーニングにムラがあり、政府の防御に負担がかかる

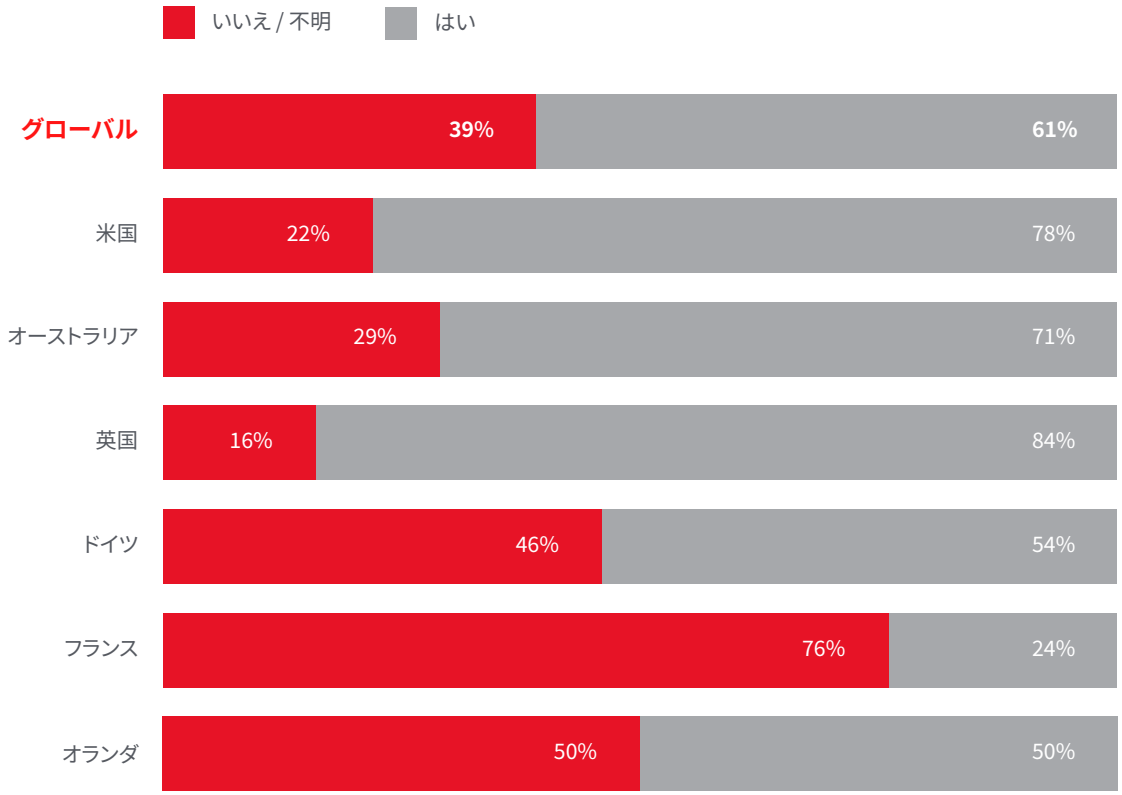
セキュリティおよび自動化技術は、最前線で強力な保護を提供しますが、セキュリティの目となり耳となるように従業員をトレーニングすることは、重要な二次防御策です。Ivanti の調査によると、公共部門におけるトレーニングは、単にすべての人に行き渡っていないだけであることがわかりました。

27%

職場でマルウェアやフィッシングなどの脅威を認識し、報告するための準備が「非常に整っている」と感じている政府職員はわずか 27% でした。

全員を対象としたトレーニング まったく違います。

Q: あなたの組織では、義務付けられたサイバーセキュリティトレーニングが実施されていますか?



重要な理由

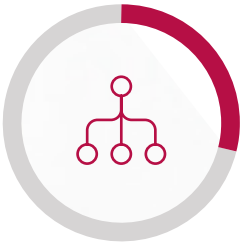
政府職員および請負業者は、義務付けられているにもかかわらず、ほとんどトレーニングが行われていないか、トレーニングが効果的ではないと報告しています

2023 Press Resetでの調査では、かなりの割合の組織でサイバーセキュリティリスクおよび報告プロセスに関する従業員の教育とトレーニングがまったく足りていないことが明らかになりました。

また、1 人がたった 1 回の過失をするだけで、予想外の壊滅的な損害を引き起こしてしまいます。政府機関の場合、そのような損害はサービスを受けるすべての国民や住民に影響を及ぼします。

32%

セキュリティ担当者が、効果的でなかったり不完全であったりする従業員トレーニングが組織のサイバーセキュリティの卓越性にとって重大な障壁であると回答しています。



29%

世界中の組織がパートナーやベンダーはサイバーセキュリティトレーニングを完了する必要がないと考えています。しかし、第三者の請負業者を利用している政府機関はリスクにさらされています。

分析結果
Press Reset: 2023サイバーセキュリティ体制の現状レポート

実世界への影響

政府機関をターゲットにした「ホエールフィッシング 101」

ホエールフィッシングは、高価値でリスクの高いターゲット、すなわち「クジラ」に対して、ソーシャルエンジニアリングのコミュニケーションを実行します。一般的なホエールフィッシングのターゲットは、事業部のリーダー、公人、財務責任者、あるいはそのアシスタントや攻撃者にとって望ましい事業部内の管理職などです。

脅威アクターは、標的を騙してコミュニケーションが本物であると信じ込ませることで、認証情報や機密情報、さらには不正な送金許可を得ることができます。

多くの場合、このようなアクセスは、検出、報告

されるまでに長い時間がかかり、高度な持続的脅威（APT）が数か月、場合によっては数年間も、政府のネットワーク内に潜んでいる可能性があります。[7]

また、調査によると、機密情報やネットワークに最も高いレベルでアクセスできる人ほど、セキュリティ習慣の意識が最も低いことが多いようです。

リーダーレベルの従業員は、他の従業員よりも安全でないセキュリティ行動を実践する可能性が高くなっています。

リーダーの 3 人に 1 人以上がフィッシングリンクをクリックした経験があります。これは一般従業員の平均の 4 倍もの割合になります。

リーダーの約 4 人に 1 人が覚えやすい誕生日をパスワードの一部に使用しています。

リーダーは、他の従業員よりもパスワードを何年も利用する可能性が高くなっています。実際に調査対象の 4 人に 1 人がそうしていました。

リーダーは、パスワードを社外の人と共有する確率が 5 倍も高くなっています。

*この統計は、公共部門を含む、あらゆる業界のリーダーに適用されます。
（プレスリセット: 2023年度サイバーセキュリティステータスレポート）

行動に移す

全職員を対象としたトレーニングの実施により、セキュリティリスクの低減と意識の向上を図ることができます。

「ホエール」（または特権ユーザー）がアクセスできる機密情報に到達するための最良の方法の 1 つは、業務上そのような人物と近くつながっている従業員を通すことであると考えられます。たとえば、次のような従業員です。

- 影響力のある重役補佐
- 受付を担当する新入社員
- 1 日中訪問している専門家の第三者の請負業者

このような人物は、正式には個人情報やストレージに直接アクセスできないものの、利便性から生まれた悪いセキュリティ慣行、そして価値の高いターゲットに近いことから、機関の最も重要な情報や資料に簡単にアクセスできる場合が多くあります。

最良のセキュリティトレーニングでは次の両方を提供します。

何を

特定の攻撃の種類、およびそれらを認識して撃退する方法

なぜ

役職、役割、場所に関係なく各従業員が担う重要な役割

次のステップ

画一的なマインドセットがない全員を対象としたトレーニング

1

アンバサダーのトレーニング

高度なトレーニングを受けた「セキュリティアンバサダー」（セキュリティ業務に携わっていないが、セキュリティに関心のある人）を育成します。

2

リスクが高い従業員には特別な注意を払う

最近の脅威をもとに、特定の政府機関の現実的なシナリオに焦点を当て、リスクの高いセグメントを特定して、それぞれにカスタムカリキュラムを開発します。

3

肯定的に接する

トレーニング内容を覚えていられるようにします。講義形式のトレーニングもありますが、競争的な活動や「ゲーム化」されたシナリオプ計画も考慮してください。

ivanti

04

将来を見据えた政府機関

ivanti

現在の問題

レガシーシステム、技術スタックの複雑さ、データサイロ、人材不足など、まだまだ続くのでしょうか。

多くの人は、政府（大都市、連邦政府機関、軍事機関、公共事業など）は、サイバーセキュリティをすべて把握しているに違いないと思い込んでいます。

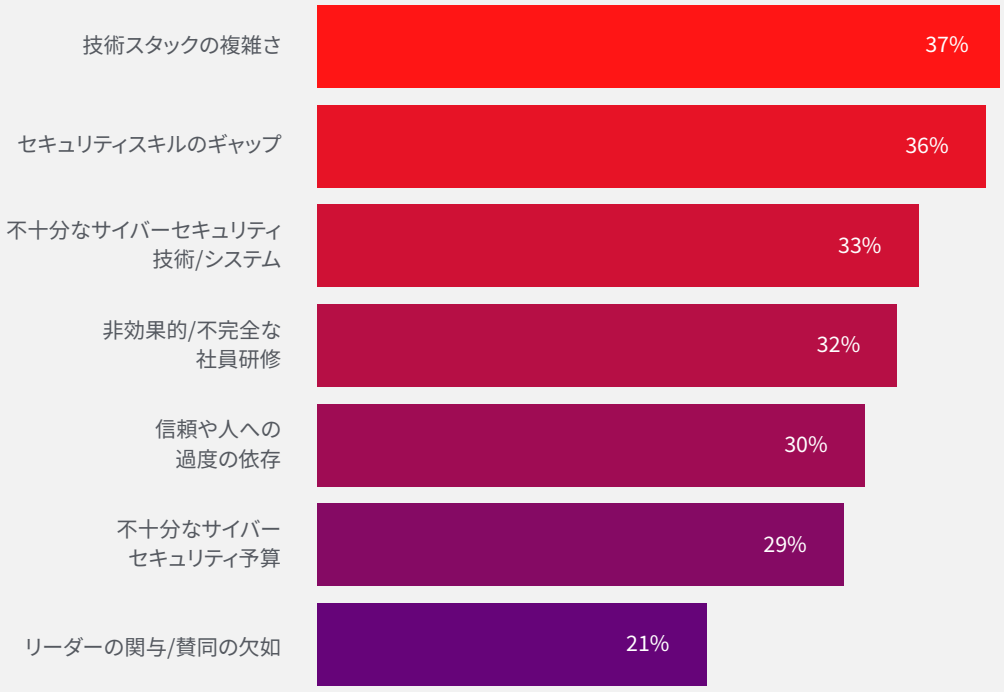
（結局のところ、最も高度なサイバーセキュリティの人材と技術の一部は、軍の部署やアプリケーションに存在しています。）

現実には、ほとんどの政府機関では、次のような項目に投資するための持続的な資金が不足しています。

- 人材
- 新しい技術
- トレーニング
- 文化

最も多く報告されたグローバルセキュリティの卓越性に対する障壁

Q: 次のうち、組織のサイバーセキュリティの卓越性を阻む大きな障壁はどれですか。



Press Reset: 2023サイバーセキュリティ体制の現状レポート

重要な理由

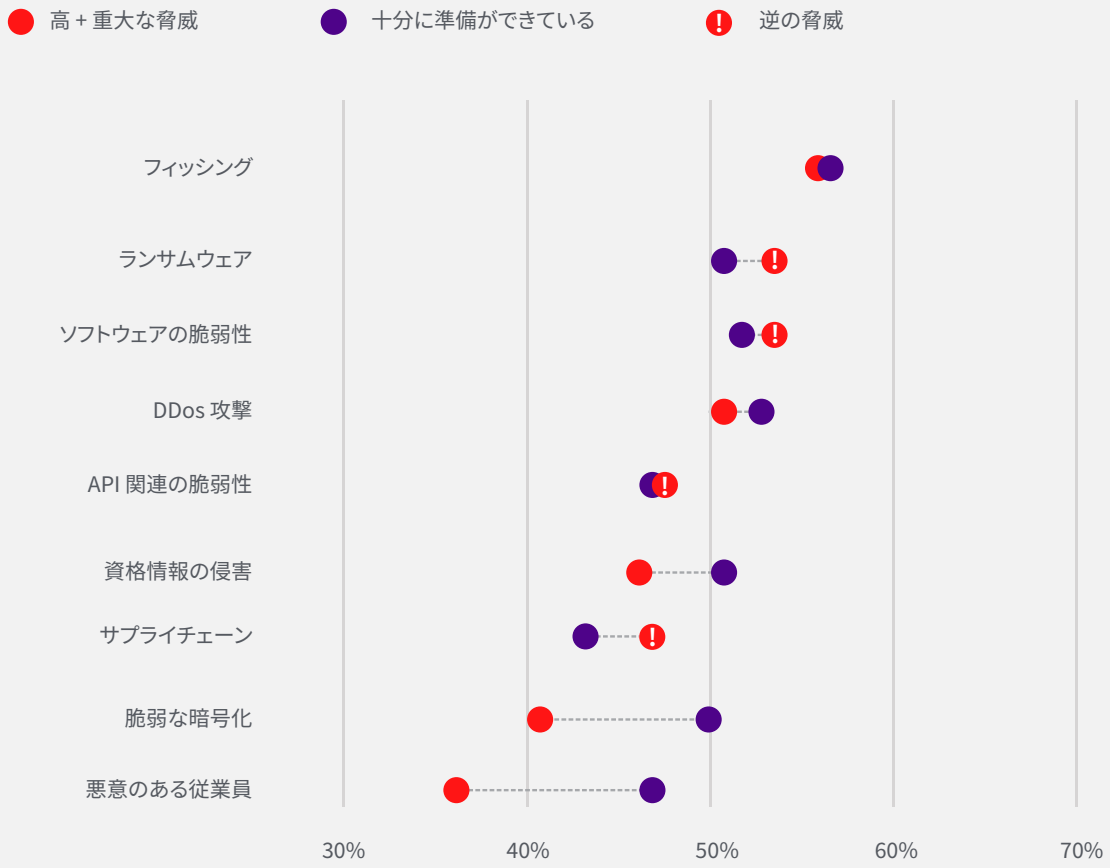
脅威アクターは、古い防御に対して武器を進化させ続けている

米国会計検査院（GAO）の報告書によると、米国連邦政府は 2010 年以降、GAO の勧告の半分以上をいまだに実行していません。[8]

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。

Q: あなたの組織は、ここに挙げた各種類の脅威に対処するために、どの程度準備が整っていますか。

セキュリティの脅威に対するセキュリティの準備



Press Reset: 2023 サイバーセキュリティ体制の現状レポート

実世界への影響

公共部門は、依然として国家が支援するハッカーにさらされている

公共部門は、国家が支援するサイバー犯罪者からの攻撃に特に脆弱です。このような攻撃者は、（どれほど物理的な距離があっても）関連する機関に対して攻撃を実行するでしょう。

右の 3 つの脅威のほか、その方法、悪用された脆弱性、公的に確認されている政府の攻撃など、より詳細な情報については、2023 年サイバー戦略ツールキットをお読みください。

「エネルギー、医療、金融の各システムは [...] すべて悪意のある主体によるサイバーリスクに直面しています。このような攻撃は、人々、環境、国家安全保障、そして最も重要な経済に対して深刻な被害をもたらす可能性があります。」[8]

Marisol Cruz Cain
GAO 情報技術・セキュリティチーム責任者

特に注目すべき世界各国政府を攻撃する高度な持続的脅威（APT）やサイバーギャングは次のとおりです。

ALPHV

「サービスとしてのランサムウェア」モデル（RaaS）の開発、販売、展開を担当するサイバー犯罪組織 。このような既製品のハッキングソリューションは、さまざまな脅威主体の能力を助長します。

APT29

スパイ活動や諜報活動に特化したロシアの対外情報機関につながる国家支援型ハッカー。

Conti

プレイブックが流出して解散したロシア系の脅威主体。しかし、Conti　系のハッカーやコードは現在でも不正な脅威となっています。Conti 型ランサムウェアの手口は、昨年も複数のサイバー犯罪者集団で顕著でした。

行動に移す

戦略的な技術と文化で、偽情報や加速する攻撃と戦う

私たちが生きている世界は、次のような偽情報が蔓延しています。

- ボットによる大規模なソーシャルメディアの偽情報キャンペーン
- 個人の嗜好に合わせた、信憑性の高いフィッシング攻撃
- 独立したジャーナリズムを弱体化させ、選挙を混乱させるディープフェイク
- 世界的な物流や医療の提供を妨害するランサムウェア

これらはすべて、公共の安全、グローバルな商取引、外交に大打撃を与え、さらには人命を奪う可能性があります。政府機関は悪意ある主体が破壊して悪用しようとするシステムやメッセージの鍵を握っているため、政府機関は特に脆弱です。

セキュリティリーダーは、戦略、システム、ツール、トレーニング、ガバナンスを開発することで、悪意のある主体を排除し、精度の高い運用を行うことで自らのポジションを守る必要があります。

そして、これらの防御を比較的に「平時」に構築することが重要です。あまりにも多くの組織が、壊滅的な攻撃を受けた後に重要な措置を講じています。

タイミングは今です。

次のステップ

技術スタックの将来を見据える

1

レジリエンス

停止時間を短縮し、影響を最小限に抑えるための対応、復旧計画を策定します。

2

自動化

自動化を導入して資産の可視性を高め、リスクに基づいた優先度を設定してパッチを適用します。どちらも 2023 年の安全な組織にとって重要な課題です。

3

エンパワーメント

サイバーセキュリティチームに、セキュリティの課題を設定するための独立性と予算を与えます。最新の脅威のニュースに軽率に反応することはやめましょう。

4

総体的なリスク管理

場所にとらわれない働き方（WFE）やハイブリッド社員、サードパーティの請負業者やベンダーなど、政府の壁を越えたセキュリティについて考えます。

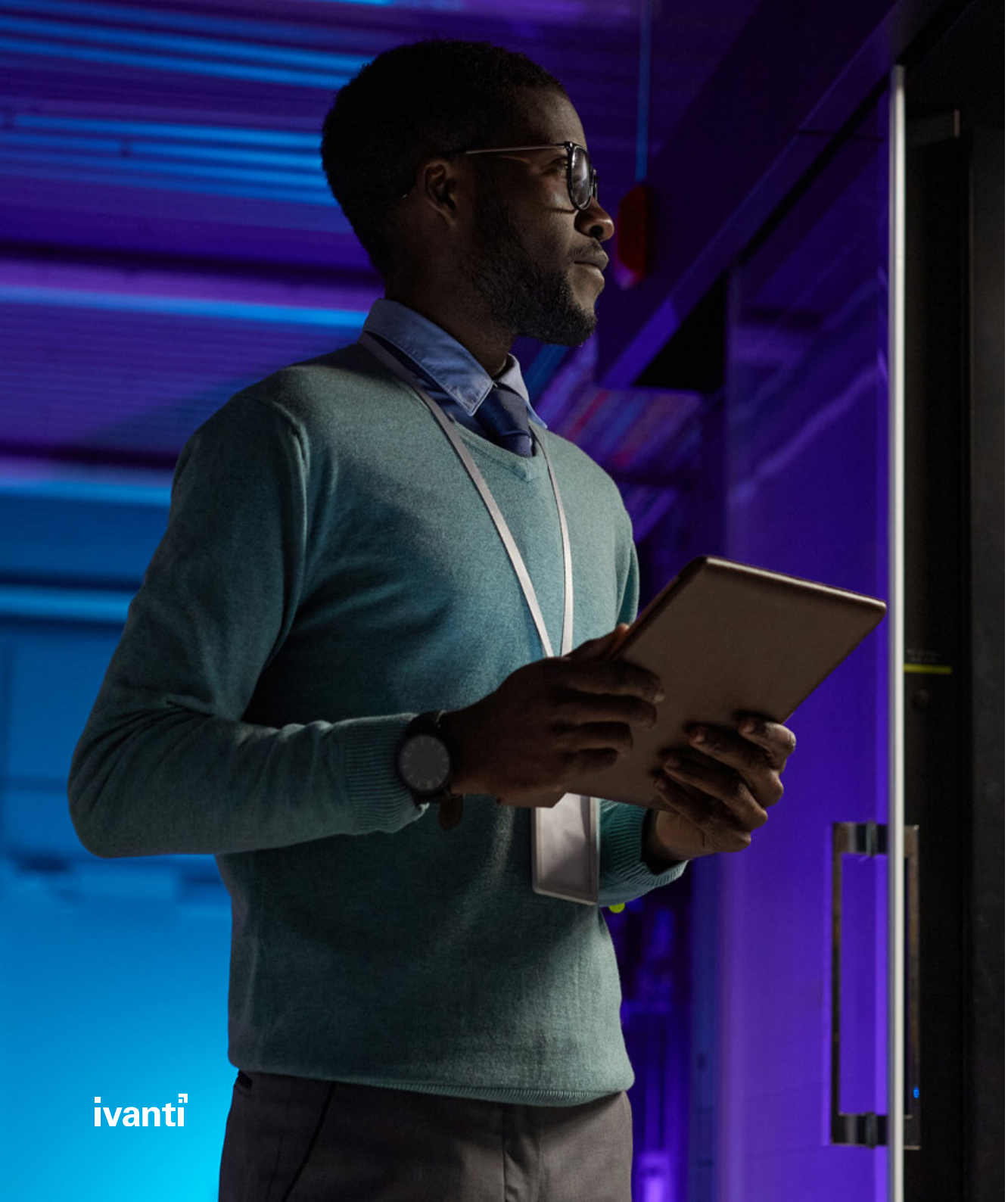
このような状況の中で、政府機関はサイバーセキュリティをチームの取り組みとして捉え、職員に負担をかけない技術でその取り組みを強化することが求められています。

職員全員がサイバーセキュリティを理解し、関心を持ち、説明責任意識を持てるようになり、より良い従業員体験を可能にする能動的なセキュリティ対策が導入されれば、政府や機関のセキュリティ態勢は強化されるでしょう。

詳細:

Press Reset: 2023サイバーセキュリティ体制の現状レポート

ivanti



参考

1. Partnership for Public Service: “Engaging employees at federal agencies,” July 14, 2022. https://ourpublicservice.org/blog/engaging-employees-at-federal-agencies/

2. Ivanti: “2023 Cyberstrategy Tool Kit for Internal Buy-in.” October 2022. https://www.ivanti.com/resources/v/doc/ebooks/ivi-2702-cybersecurity-tool-kit-internal-buy-in-budget-influence-non-infosec

3. Sharon Ben-Moshe, Gil Gekker, Golan Cohen / Check Point Research: “OPWNAI: AI That Can Save the Day or Hack It Away.” Dec. 19, 2022. https://research.checkpoint.com/2022/opwnai-ai-that-can-save-the-day-or-hack-it-away/

4. VOA: “Research: Deepfake ‘News Anchors’ in Pro-China Footage.” Feb. 8, 2023. https://www.voanews.com/a/research-deepfake-news-anchors-in-pro-china-footage/6953588.html

5. U.S. Government Accountability Office: “Cybersecurity High-Risk Series: Challenges in Protecting Privacy and Sensitive Data,” Feb. 14, 2023. https://www.gao.gov/products/gao-23-106443

6. Partnership for Public Service: “Employee Engagement,” July 13, 2022. https://ourpublicservice.org/our-solutions/employee-engagement/
Federal News Network: “Return-to-office plans a major cause for decline in 2021 Best Places to Work results,” July 13, 2022. https://federalnewsnetwork.com/workforce/2022/07/return-to-office-plans-a-major-cause-for-decline-in-2021-best-places-to-work-results/

7. Ivanti: “2023 Cyberstrategy Tool Kit for Internal Buy-in.” October 2022. https://www.ivanti.com/resources/v/doc/ebooks/ivi-2702-cybersecurity-tool-kit-internal-buy-in-budget-influence-non-infosec

8. U.S. Government Accountability Office: “Cybersecurity High-Risk Series: Challenges in Establishing a Comprehensive Cybersecurity Strategy and Performing Effective Oversight,” Jan. 19, 2023. https://www.gao.gov/assets/gao-23-106415.pdf

政府系サイバー セキュリティ現状レポート

2023年に取り組むべき行動と変化の推進の指針となる４つの重要なポイント

ivanti

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