FORTINET
Training Institute

サイバーセキュリティスキルギャップレポート 2024 年版

グローバル調査
レポート

目次

3 調査方法

4 概要

5 サイバーセキュリティに求められる全員参加のアプローチ

7 企業幹部への責任追及

11 侵害による貴重な時間と資金の損失

17 サイバーセキュリティを左右する 3 つの要因

21 認定資格を持つ候補者の優位

25 実績を過小評価されている候補者の見落とし

29 終わりに

30 フォーティネットについて

調査方法

本レポートの調査結果は、1,855 人の IT およびサイバーセキュリティ関連の意思決定者を対象に、2024 年 1 月に Sapio Research が実施したオンラインインタビューならびに E メールでの調査から得た回答に基づいています。調査およびインタビューは次の 29 ヵ国 / 地域で実施されました。

- アルゼンチン
- オーストラリア
- ブラジル
- カナダ
- コロンビア
- フランス
- ドイツ
- 香港
- インド
- インドネシア
- イスラエル
- イタリア
- 日本
- 中国
- マレーシア
- メキシコ
- オランダ
- ニュージーランド
- フィリピン
- シンガポール
- 南アフリカ
- 韓国
- スペイン
- スウェーデン
- 台湾
- タイ
- アラブ首長国連邦
- 英国
- 米国

結果全体の精度は 95% 信頼区間で許容誤差± 2.3% です。

企業規模

従業員数 100 ～ 499 人：**24%**
従業員数 500 ～ 999 人：**23%**
従業員数 1,000 ～ 2,499 人：**21%**
従業員数 2,500 ～ 4,999 人：**17%**
従業員数 5,000 人以上：**14%**

性別

男性：**68%**
女性：**32%**

回答者総数：1,850 人

アジア太平洋地域：**30%**
欧州 / 中東 / アフリカ：**27%**
北米：**22%**
中南米 / メキシコ：**22%**

役職

企業の代表者：**13%**
経営幹部レベル（C レベル）の管理職：**34%**
副社長職：**9%**
本部長職：**11%**
部長職：**33%**

ビジネスセクター トップ 3

テクノロジー：**21%**
製造：**15%**
金融サービス：**13%**

概要

2024 年のサイバーセキュリティの状況は、組織にとってリスクが高いといえます。セキュリティ侵害による金銭的被害が続いているうえ、侵害が発生した場合には経営幹部が罰則を科されます。組織は対応策として、訓練、意識向上、テクノロジーを組み合わせた 3 本柱のサイバーセキュリティアプローチに注目しています。

企業幹部への責任追及

51% の回答者が、サイバー攻撃を受けて取締役や経営幹部が罰金、禁固、罷免、解雇などの処分を受けたと回答

サイバーセキュリティ強化のために取締役会が検討または実施した対策：

- IT / セキュリティ担当者に対する研修または資格取得の義務化：**64%**
- 全従業員向けのセキュリティ意識向上トレーニング：**61%**
- セキュリティソリューションの購入：**59%**

72% の回答者が、2023 年はサイバーセキュリティに対する取締役会の注目度が前年度よりも高まったと回答

侵害による貴重な時間と資金の損失

87% の回答者が、2023 年にセキュリティ侵害が 1 回以上発生したと回答

63% の回答者がサイバー攻撃からの復旧に 1 ヵ月以上を要したと回答

53% の回答者が、侵害による減益、罰金、その他の費用が 100 万ドル以上に上ったと回答（2022 年 の 48%、2021 年 の 38% から増加）

サイバーセキュリティを左右する 3 つの要因

IT リーダーが回答した侵害の原因トップ 3：

- IT / セキュリティスタッフのスキルおよびトレーニング不足：**58%**
- 組織または従業員のセキュリティ意識の欠如：**56%**
- サイバーセキュリティ製品の不備：**54%**

70% の回答者はサイバーセキュリティのスキル不足によって組織のリスクが増大すると回答

61% の IT 意思決定者は、最大の課題はネットワークエンジニアリングおよびセキュリティ分野の経験を持つ人材の獲得であると回答

認定資格を持つ候補者の優位

91% の回答者が認定資格を持つ候補者を優先的に採用

89% の回答者が従業員のサイバーセキュリティ認定資格取得に費用を支給する考え

72% の回答者は、テクノロジー関連の認定資格を持つ候補者を見つけるのが困難と回答（2022 年の 73% から微減、2021 年の 78% から減少）

実績を過小評価されている候補者の見落とし

83% の企業が今後 2 ～ 3 年間のダイバーシティ採用目標を設定

72% が 4 年制学位を必要条件とし、**66%** は従来型の教育課程終了者のみを採用

継続的目標をよそにダイバーシティ採用は年々変化：

- 女性の積極採用は 2022 年の 89%、2021 年 の 88% から **85%** に減少
- マイノリティグループからの積極採用は **68%** で変化なし、2021 年の 67% から微増
- 退役軍人の積極採用は **49%** で、2022 年 の 47% から若干増加するも 2021 年の 53% からは減少

はじめに

サイバーセキュリティに求められる全員参加のアプローチ

「サイバーセキュリティスキルギャップレポート 2023 年版」では、取締役会のサイバーセキュリティに対する関心が高まっていることをお伝えしました。さらに理解を深めるための新たな設問は、現在の状況の原因を解明し、サイバー脅威に対抗するため企業が進めつつある総合的アプローチを明らかにします。

本レポートを作成するにあたり、私たちはビジネスリーダーの優先事項、脅威情勢、サイバーセキュリティ戦略、認定資格の価値、多様な人材プールからの採用という 5 つの視点からサイバーセキュリティスキルの課題を検証しました。

その結果、大きな損害を伴うサイバー攻撃がますます頻発し、取締役や管理者個人への深刻な影響もあり得ることからサイバー防御の強化が急務となり、それがトップダウンで進められていることが明らかになりました。

今年のレポートは、一部の設問では 2021 年まで遡って比較統計を示すと共に、重要なトピックを深く掘り下げることで、スキルギャップの現状を詳細かつ全体的に考察しています。また、サイバーセキュリティに対する取締役レベルの見解についての追加情報や、侵害の影響に関する新しいデータ、そうした影響に対する組織の対応計画なども取り上げています。

一部の課題が解決されず、根強く残っていることは明らかです。サイバーセキュリティのスキルギャップは、今もなお業界に損失をもたらしています。さらに、ほとんどの回答者は、必要なスキルセットを持つ従業員の採用と定着に依然として苦労しています。その原因の一端は、非従来型の人材プールをいまだに活用できていないことや、「因習的な」資格を必要条件としていることにあるかもしれません。

重要なポイントは、実効性のあるサイバーセキュリティには、以下の 3 本柱のアプローチが必要であるということです。

1. **IT およびセキュリティチームへの支援**：目標の達成に必要なトレーニングと認定資格取得に投資することで、不可欠なサイバーセキュリティスキルを確保します。
2. **第一線で働くスタッフのサイバーセキュリティ意識の向上**：これらのスタッフは防御の最前線としてセキュリティに貢献できます。
3. **効果的なサイバーセキュリティソリューションの入手と利用**：強固なセキュリティ態勢を整えます。

51% の組織が、サイバー攻撃を受けて経営幹部が罰金、禁固、罷免、解雇などの処分を受けたと回答

企業幹部への責任追及

今日の取締役会ではサイバーセキュリティへの関心が高まっており、それは個人的な動機による関心である可能性もあります。半数余り（51%）の回答者は、サイバー攻撃を受けて取締役や経営幹部が罰金、禁固、罷免、解雇などの処分を受けたと回答しています。

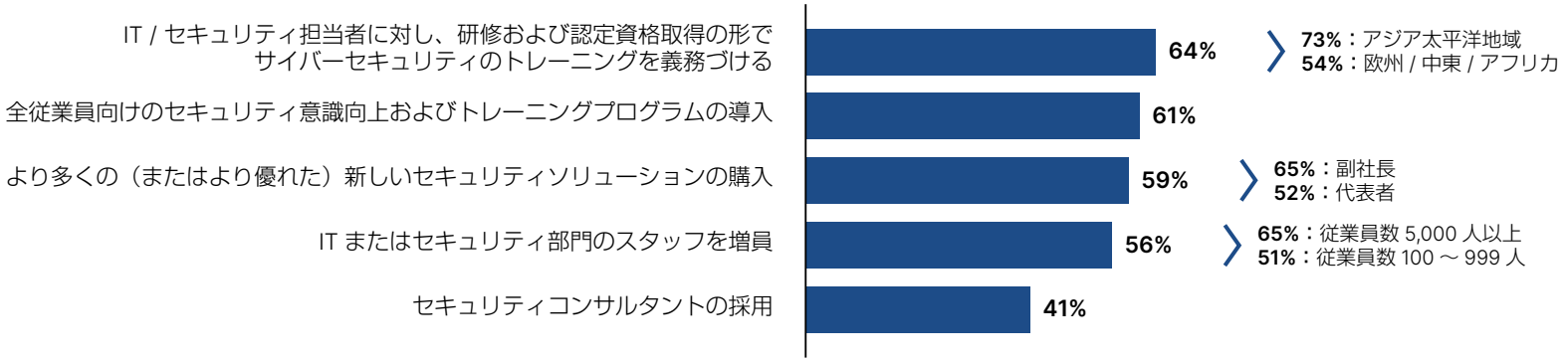
そのようなリスクを考えると、約 3 / 4（72%）の回答者が、2023 年はサイバーセキュリティに対する取締役会の注目度が前年度よりも高まったと答えたのも不思議ではありません。取締役会で検討または実施された改善策としては、IT / セキュリティ担当者に対する研修または認定資格取得の義務化（64%）、全従業員向けのセキュリティ意識向上トレーニング（61%）、より多くの（またはより優れた）新しいセキュリティソリューションの購入（59%）が挙げられます。

これらの改善策は、スキルや訓練されたスタッフ、さらにはセキュリティ意識や製品の不足がセキュリティ侵害の主な原因であるという IT リーダーの見解と合致しています。詳細については17 ページを参照してください。

取締役会のサイバーセキュリティの優先事項：トレーニング、意識向上、ソリューション

取締役は、知識、スキル、セキュリティ意識は堅固なサイバー防御の重要な第一線であること、そして、それらを後方支援するためにテクノロジーが不可欠であることを認識しているようです。

検討または実施された改善策



詳細報告

取締役会はサイバーセキュリティをビジネスの至上命題と認識

取締役会によるサイバーセキュリティへの取り組み

昨年は、93% の回答者が取締役会でサイバー防御に関する質問が出ると答えました。今年の調査では、取締役会がサイバーセキュリティのどの部分を重要視しているかを詳しく調べています。

- 97% の回答者は、取締役会がサイバーセキュリティをビジネスの優先事項と考えていると回答しました。
- 56% は、取締役会が IT / セキュリティスタッフの増員を検討または実施したと回答しました。

リーダーは組織の規模を問わずペナルティに直面

取締役や経営幹部が罰則を受けるリスクはすべての組織でほぼ同じです。

- 最も高リスクな従業員数 2,500 ～ 4,999 人の組織の場合、39% がサイバー攻撃を受けて経営幹部が罰則を受けたと報告しました。
- 中小企業（従業員数 100 ～ 999 人）の 31%、大企業（従業員数 5,000 人以上）の 32% も、経営幹部に罰則が科されたと回答しています。

リーダーに対する最も一般的な罰則は罰金

サイバー攻撃後、責任を問われた取締役や経営幹部の大半は罰金を科されましたが、それ以外にも重大な決定が下されました。

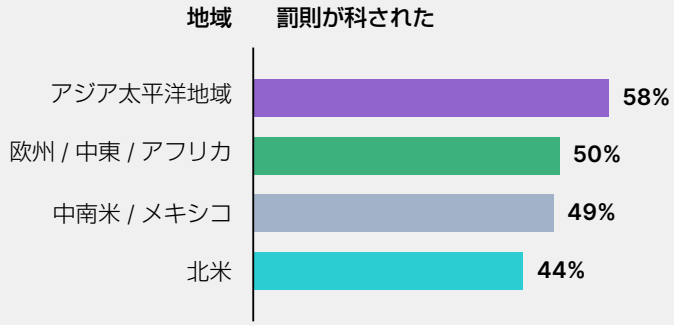
- 罰金刑：34%
- 罷免または解雇：33%
- 実刑：16%

97% の回答者が、取締役会はサイバーセキュリティをビジネスの優先事項と考えていると回答

地域別特徴

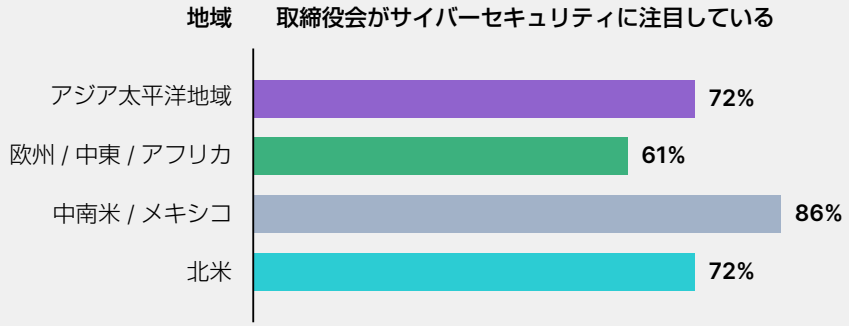
経営幹部が処罰された割合が最も高いのはアジア太平洋地域

アジア太平洋地域の経営幹部や取締役は、サイバー攻撃後に罰金刑、禁固刑、罷免、または解雇に処された割合が最も高くなりました。



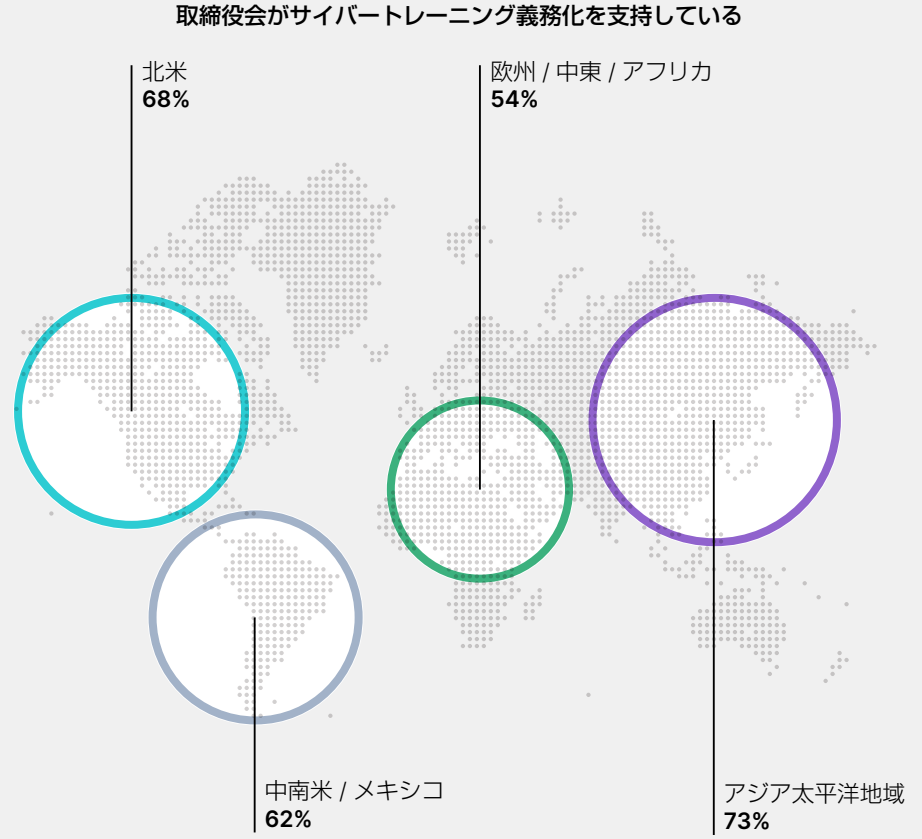
取締役会のサイバーセキュリティへの注目度が最も高い地域は中南米

前年と比較して、取締役会のサイバーセキュリティへの注目度は中南米が最も高く、最も低いのは欧州 / 中東 / アフリカです。



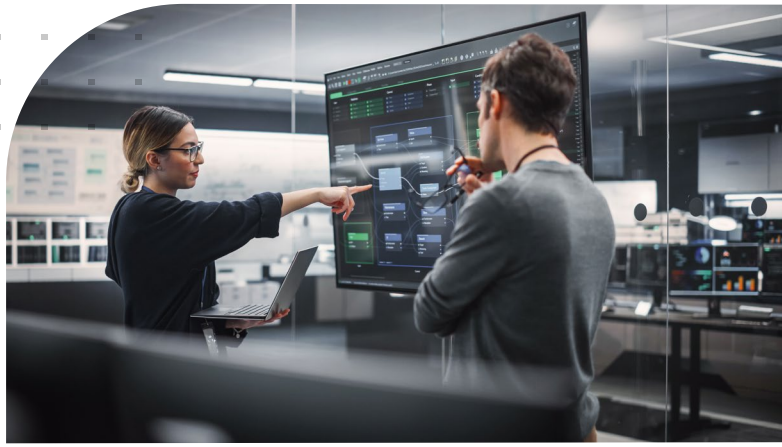
アジア太平洋地域の取締役会はサイバーセキュリティトレーニングの義務化を支持

IT およびセキュリティ担当者へのサイバートレーニングの義務化は、アジア太平洋地域で取締役会の支持が最も高く、欧州 / 中東 / アフリカで最も低くなりました。



53% の回答者が 2023 年の侵害によるコストを **100 万ドル**超と回答

侵害による貴重な時間と資金の損失



大多数（87%）の組織は、2023 年にセキュリティ侵害が 1 回以上発生したと回答しました。そのうち、減益、罰金、その他の費用が 100 万ドルを越えた組織は半数以上（53%）に上り、2022 年の 48%、2021 年の 38% から増加しています。

2023 年に侵害がまったくなかったと答えた組織はわずか 13% で、2022 年は 15%、2021 年は 20% でした。侵害による金銭的被害も増大しているようです。今年の回答者のうち、サイバー攻撃による出費が発生しなかったと答えた組織はわずか 17% で、2022 年の 21%、2021 年の 36% から減少しました。

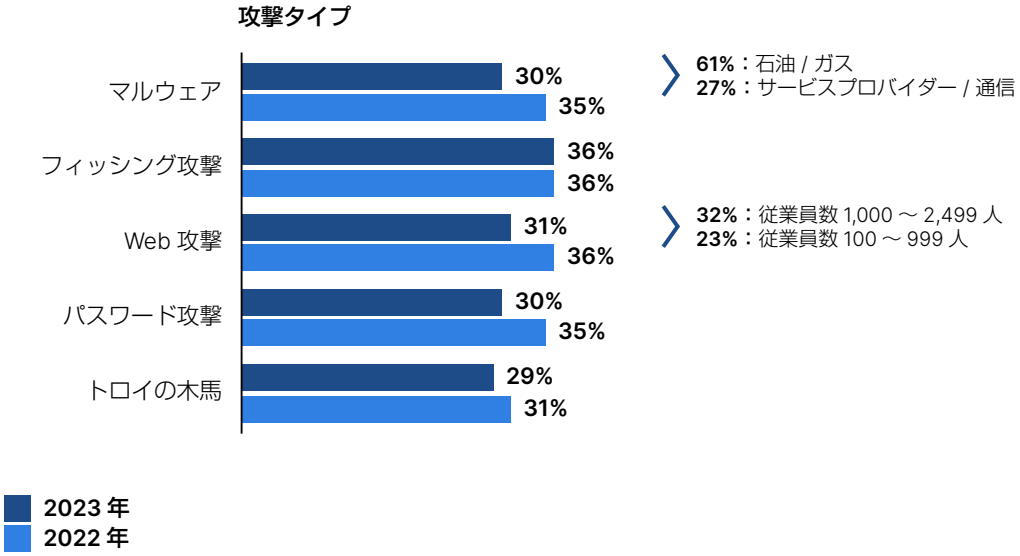
回答者の報告によると、侵害はさまざまなタイプの攻撃によってもたらされています。マルウェア、フィッシング、および Web 攻撃を合わせると、年間を通じて全攻撃の 80% を占めています。頻繁に使用されている攻撃タイプの多くは、個人ユーザーを直接標的にしており、一般社会におけるセキュリティ意識の重要性がはっきりと表れています。

1 件以上のサイバーセキュリティ侵害

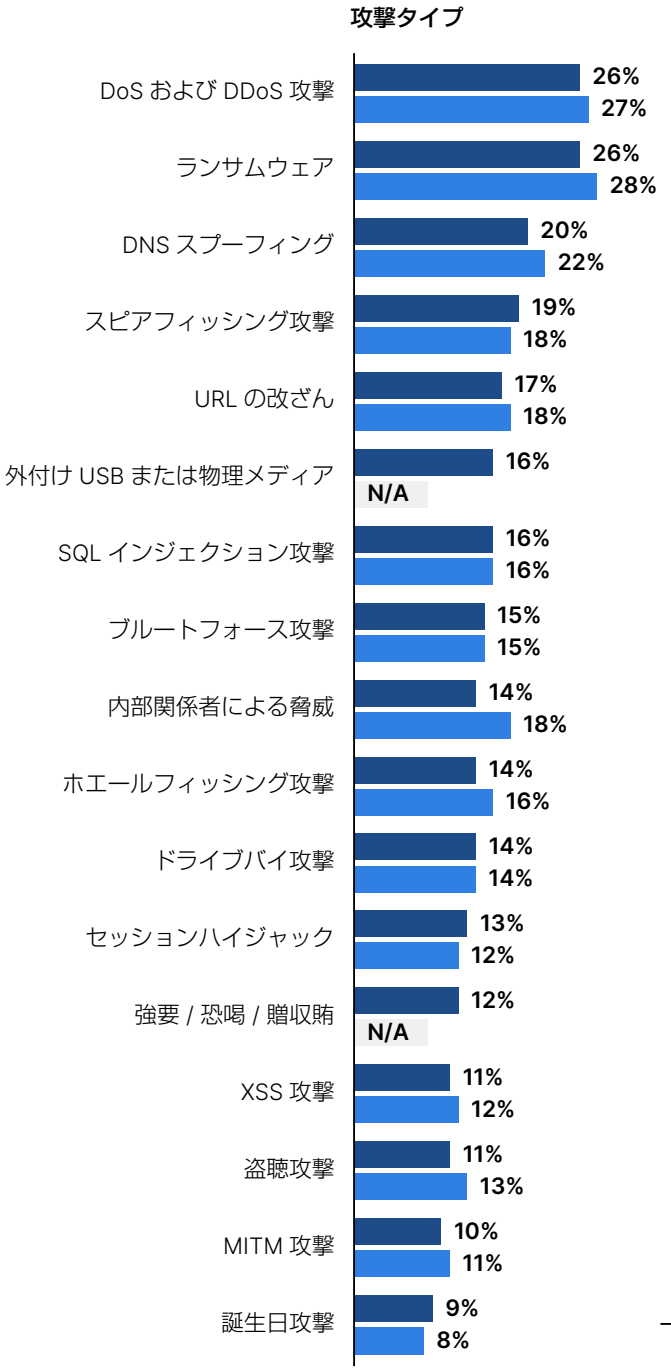
マルウェア、フィッシング、およびWeb攻撃は、年間を通じて全攻撃の**80%**を占める

既知の脅威情勢

2023 年に最も多く発生した攻撃のトップ 5 は昨年と変わらず、マルウェア、フィッシング攻撃、Web 攻撃、パスワード攻撃、トロイの木馬です。



2023 年の調査では、外付け USB または物理メディア攻撃（16%）と強要 / 恐喝 / 内部スタッフによる贈収賄（12%）が攻撃タイプに追加されました。



詳細報告

攻撃からの復旧は困難

復旧は多大な時間を要する

回答者の平均復旧期間は約 3（2.7）ヵ月でした。

- 過半数（63%）の組織は、サイバー攻撃からの復旧に 1 ヵ月以上を要しました。
- 35% は 1 ～ 3 ヵ月、
- 約 1 / 3（28%）は 4 ヵ月以上かかっています。

企業は攻撃の件数と頻度が増加すると予測

攻撃の激化と影響の拡大を念頭に、ほとんどの回答者は事態が好転する前に悪化すると予測しています。

- 80% は今後 1 年間でサイバー攻撃が増加すると予測しています（2022 年の 65% から増加）。
- 攻撃がどの程度増加すると思うかという設問には、平均して、今後 12 ヵ月間で 19.3% の増加を予測していると回答しました。これは、平均値が 20% だった 2022 年とほぼ同じです。

事業の規模と分野が攻撃を助長

特定の規模と業種の企業で、複数のサイバー攻撃が発生している傾向が見られます。

- 従業員数 1,000 ～ 2,499 人の企業は、35% が過去 12 ヵ月間に 5 回以上の攻撃を受けたと回答しており、2022 年の 29% から増加しました。
- 従業員数 2,500 ～ 4,999 人の企業も、同じく 35% が 5 回以上の攻撃を報告しており、昨年の 30% から増加しています。
- 全業種の中で複数の攻撃が最も多かったのは石油 / ガス企業で、56% が 5 回以上の攻撃を報告しています（昨年の 31% から増加）。

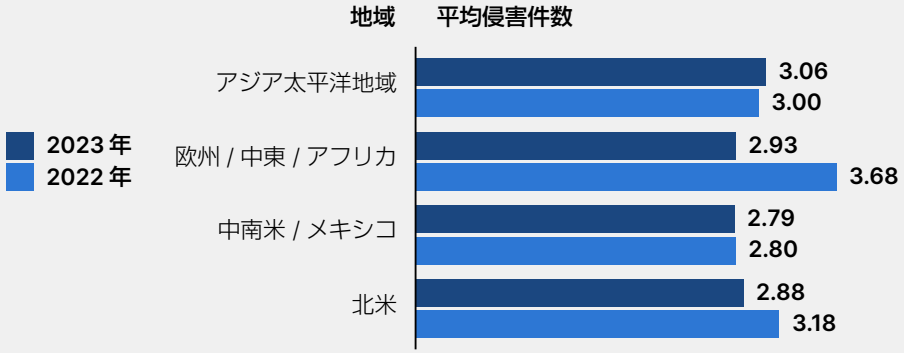
攻撃からの平均復旧期間は

2.7 ヵ月

地域別特徴

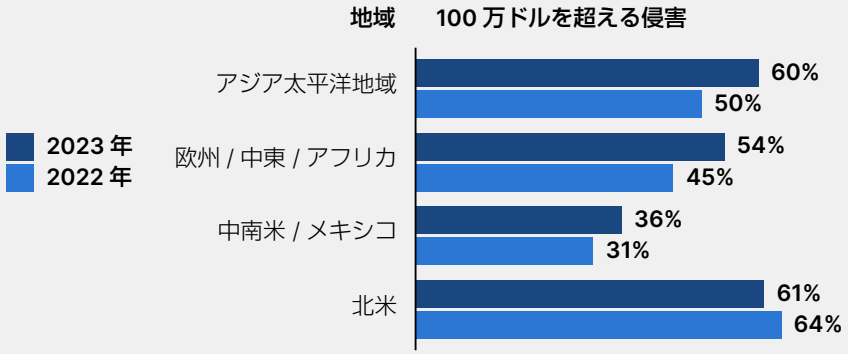
侵害は世界中で同様に発生

平均侵害件数はアジア太平洋地域でやや多く、中南米 / メキシコで若干少ないものの、すべての地域で拮抗しています。



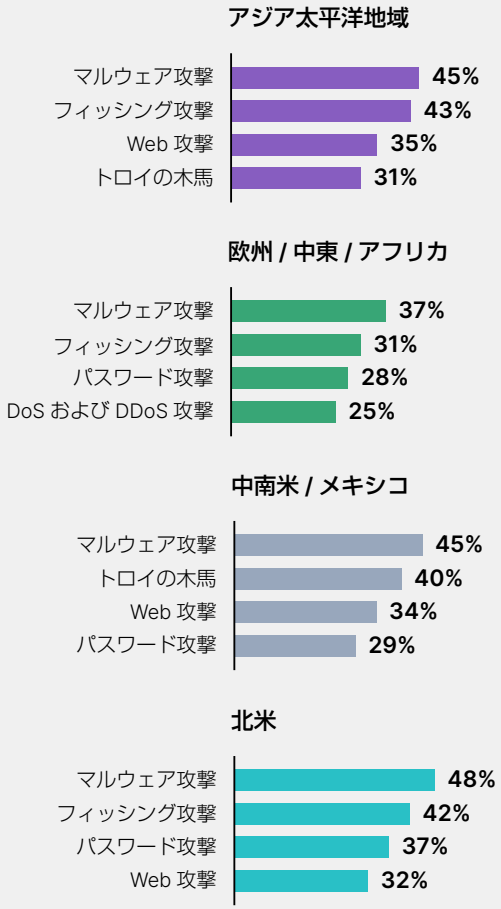
北米とアジア太平洋地域は攻撃のコストが高額

金銭的被害は、依然として北米とアジア太平洋地域が最も大きく、2023 年のコストは 100 万ドルを超えています。北米を除くすべての地域で、高額なコストを伴う攻撃が 2022 年よりも増加しています。



上位攻撃タイプには多少の地域差

マルウェア攻撃は、すべての地域で最もよく見られた攻撃タイプです。北米では、パスワード攻撃が他地域よりも多く発生しました。アジア太平洋地域では、フィッシング攻撃と Web 攻撃が他地域よりも多くなっています。



58% の IT 意志決定者は、セキュリティ侵害の主な原因を IT / セキュリティスタッフのサイバーセキュリティスキルおよびトレーニング不足と回答

サイバーセキュリティを左右する 3 つの要因

格言にもあるように、知識は力です。裏を返せば、知識の欠如は弱点と見なされ、特にサイバーセキュリティでは大きな不利益になります。半数以上（58%）の回答者は、IT / セキュリティスタッフのスキルおよび訓練不足が侵害の主な原因であると回答しています。さらに、56% が組織または従業員のセキュリティ意識の欠如、54% は必須のサイバーセキュリティ製品の不備を原因に挙げました。

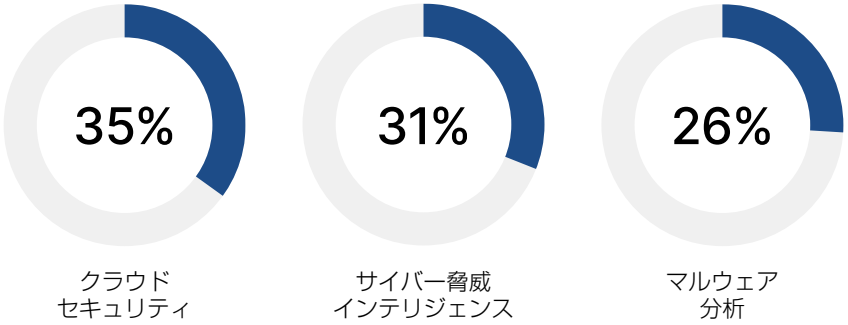
技術的スキル、スタッフ、セキュリティソリューションが主な要因と考えられているとすれば、65% の IT リーダーが、サイバー攻撃に対応して IT / セキュリティチームの増員を計画していると回答するのも理解できます。

これとほぼ同数（62%）のリーダーは、IT およびセキュリティ担当者に対し、認定資格の取得という形でサイバーセキュリティトレーニングを義務づけると回答しました。同じくほぼ同数（61%）が、全従業員向けのセキュリティ意識向上およびトレーニングプログラムを導入すると回答し、過半数（59%）のリーダーは、より多くの（またはより優れた）新しいセキュリティソリューションの購入も計画しています。

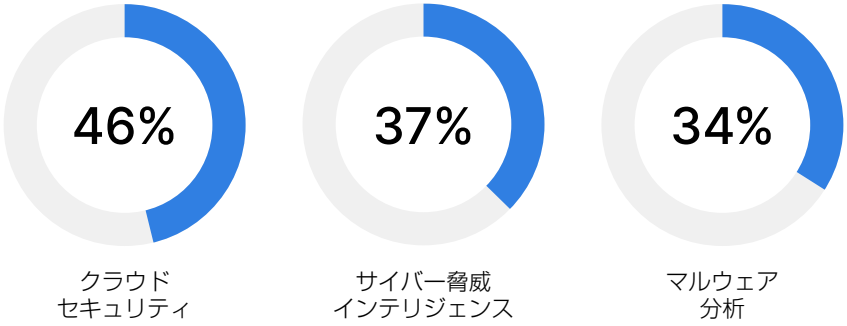
需要の高いスキルは変化なし

調査に参加したすべての組織において、需要の高いサイバーセキュリティスキルのトップ 3 は 2022 年と 2023 年で同じでした。割合の変化に影響したかどうかは不明ですが、2023 年のリストには前年の調査になかった新しいスキルが追加されています。

2023 年に最も必要とされたスキル



2022 年に最も必要とされたスキル



詳細報告

サイバーセキュリティには人材が不可欠

スキル不足は不利益

70% の回答者は、サイバーセキュリティのスキル不足によって組織のリスクが増大すると回答しており、2022 年の 68%、2021 年の 67% からやや増加しました。

- 61% の回答者は、ネットワークエンジニアリングとセキュリティ分野の経験を持つ候補者を見つけるのが難しいと回答しました。
- 補充が最も困難な職種は、引き続きセキュリティオペレーションとクラウドセキュリティ（43%）で、どちらの職種も 2022 年の 44% から若干減少しました。

採用難は供給の問題

人材確保は容易になりつつあるとはいえ、課題はいまだ残っています。

- 54% の組織は、サイバーセキュリティ人材の採用に苦労していると答えました。2022 年の 56%、2021 年の 60% からは数値が若干減少しましたが、半数以上の回答者にとって、サイバーセキュリティの専門知識を持つ候補者の確保が課題であることに変わりはありません。
- 51% の回答者は、必要なスキルセットの人材プールが総じて不十分であると答えています。

従業員は知識の習得と成長を望んでいる

従業員はトレーニングやスキルアップに高い価値を感じているため、人材を定着させる苦労は多少緩和されつつあります。

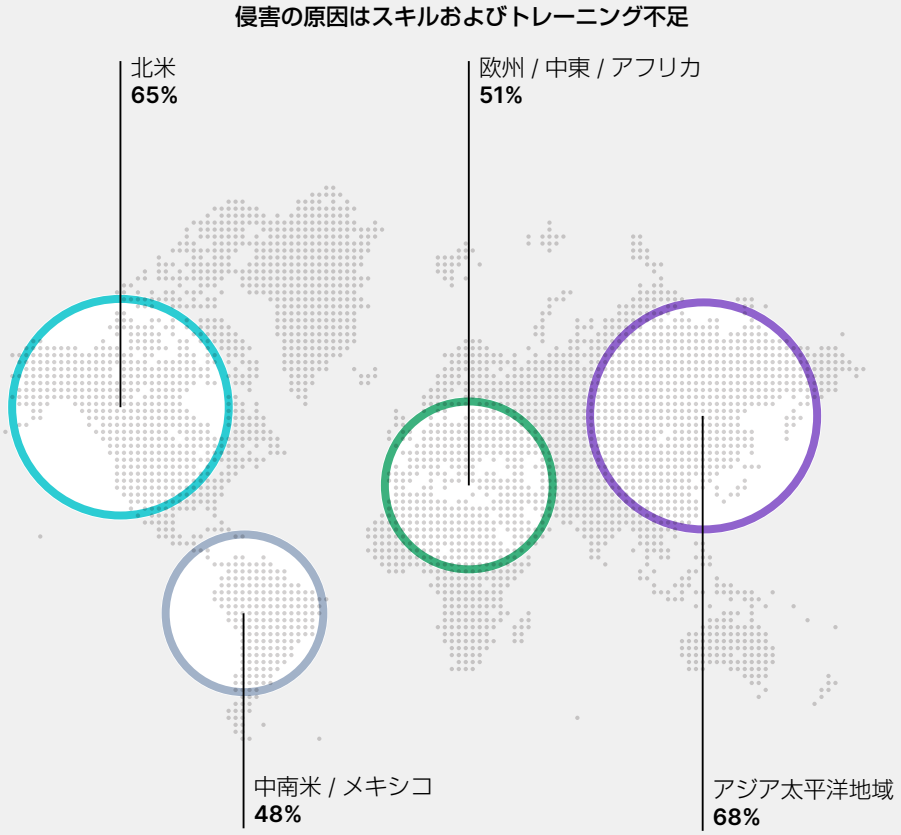
- サイバーセキュリティ人材の定着に苦労していると答えた組織は 50% で、2022 年（54%）と 2021 年（52%）からわずかに減少しました。
- 人材定着における最大の課題は、組織が十分なトレーニングとスキルアップの機会を提供できていない点です（50%）。
- 給与 / 福利厚生（41%）とリモート / ハイブリッドワークへの対応（38%）は、それほど大きな問題にはなっていません。

50% の回答者が、人材定着における最大の課題はトレーニングとスキルアップの機会の欠如であると回答

地域別特徴

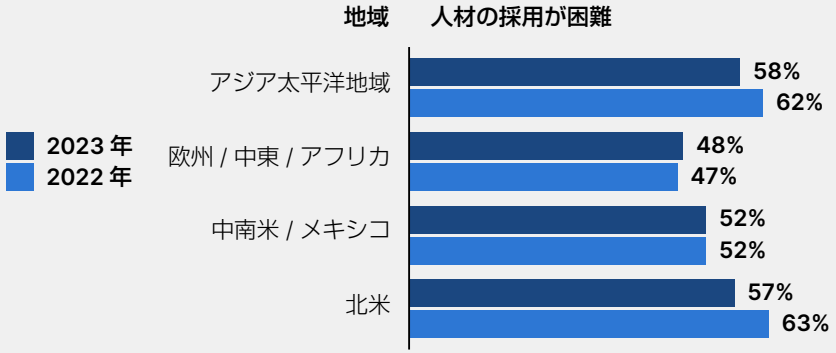
侵害とスキルの関連性はアジア太平洋地域が最高

アジア太平洋地域では、68% の企業がサイバーセキュリティのスキルおよびトレーニング不足を侵害の原因としているのに対し、中南米 / メキシコではわずか 48% です。



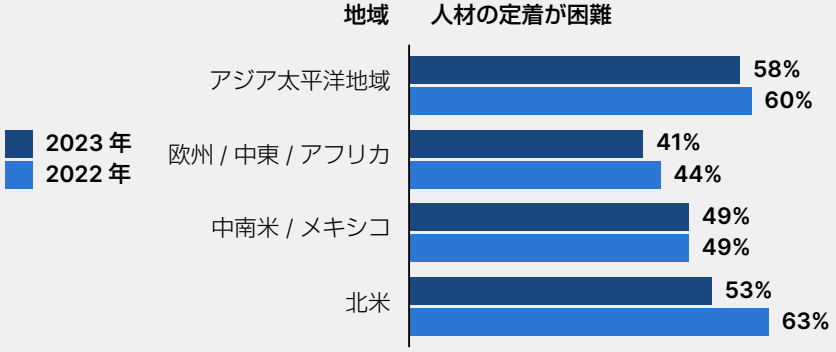
採用に最も苦労しているのはアジア太平洋地域と北米

割合に多少の変化はありますが、この状態は 2022 年から変わっていません。



アジア太平洋地域の企業は人材の定着に苦慮

北米の組織では、2022 年と比べて人材定着の問題が大きく緩和されました。欧州 / 中東 / アフリカではやや緩和され、中南米 / メキシコでは変化はありません。



91% のリーダーが
有資格者を優先的に採用

認定資格を持つ候補者の優位

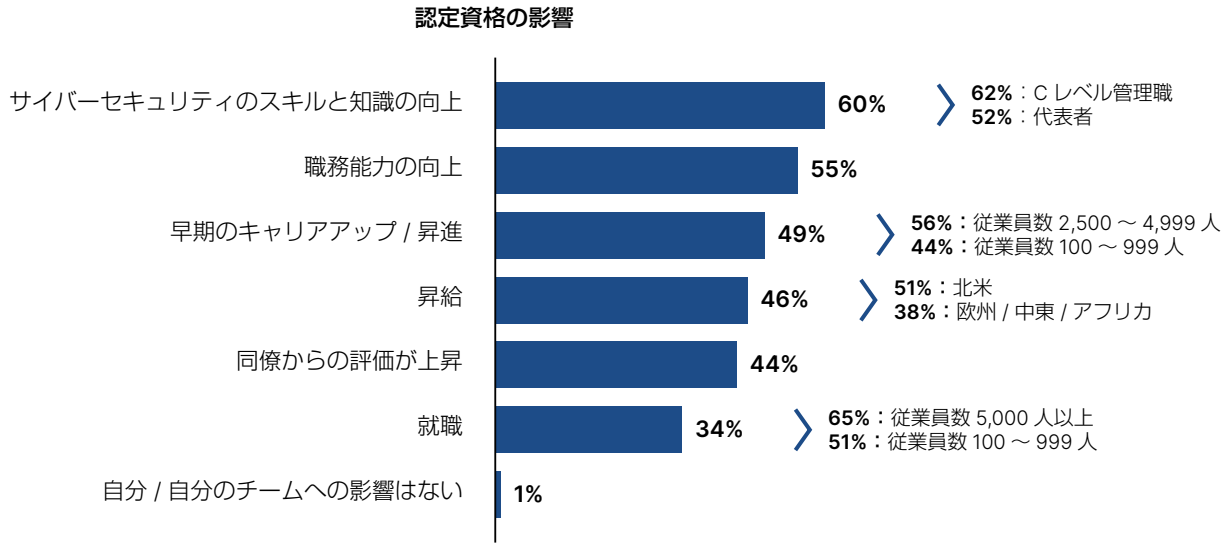
IT リーダーは、サイバーセキュリティの専門知識を証明するものとして、認定資格を非常に重要視しています。ほぼすべて（91%）の IT リーダーが、認定資格を持つ候補者を優先的に採用しています。この数字は 2022 年と同じで、2021 年の 10% からは増加しています。過半数（67%）の回答者は、チームのメンバーや直属の部下が認定資格を保持していることを希望しています。そうした実績はサイバーセキュリティに対する高い意識や専門知識を証明すると考えているからです。

認定資格への需要は高いものの、72% の回答者はテクノロジー関連の認定資格を持つ候補者を見つけるのが難しいと答えています。この割合は 2022 年（73%）とほぼ同じですが、2021 年の 78% からは減少しており、資格を持つ人材を多少は見つけやすくなっていることを示しています。

89% の IT リーダーは、従業員のサイバーセキュリティ認定資格取得に費用を支給すると答えています。「支給する」と答えた割合は、過去 3 年間、高い数値で比較的安定しています（2022 年は 90%、2021 年は 91%）。

認定資格による多大な効果

認定資格保持者、あるいは認定資格保持者と共に働く人は、明確な利点を理解しています。それらの利点の最上位に、スキルと知識の向上があります。



詳細報告

認定資格が信頼を醸成

IT リーダーは認定資格の価値を身をもって知っている

回答者の 84% は、自身が認定資格を保持しています。この割合は 2022 年と同じで、2021 年（86%）とも近い数値です。

- チームに有資格者が含まれる回答者は 85% で、昨年から 1% 減少、2021 年（88%）からもわずかに減少しました。
- 3 年にわたって認定資格に関する回答率が比較的安定しているのは、個人および組織が認定資格の重要性を認識していることを示唆しています。

認定資格はセキュリティ意識と専門知識を向上させる

67% の回答者は、認定資格によってサイバーセキュリティに関する高い意識と専門知識が証明されると答えています（2022 年の 68% とほぼ同じ）。

- 57% は、セキュリティベンダーの製品に精通していることを認定資格によって証明できると回答しました（2022 年の 54% から増加）。
- 認定資格の取得が業務に影響しないと答えた回答者はわずか 1% でした。

認定資格はセキュリティ態勢を強化する

61% の回答者は、認定資格保持者の方が、進化するセキュリティ情勢への対応に優れていると回答しました。これは 2022 年の 66% から若干減少しましたが、2021 年の 42% よりも増加しています。

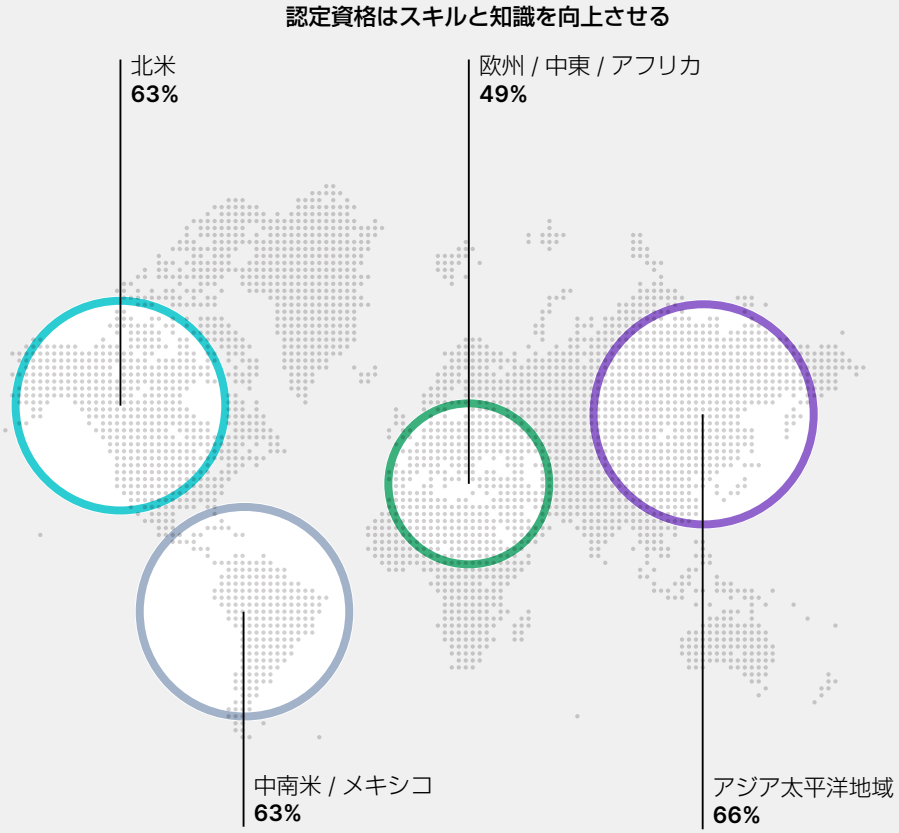
- これらの回答者のうち、70% は組織へのサイバー攻撃が過去 1 年間に 9 回以上、59% は 1 ～ 4 回と回答しています。
- こうした相関関係は、サイバー攻撃対策の責任者が認定資格を重視していることを示唆しています。

認定資格は進化するセキュリティ情勢への個人の対応能力を向上させると **61%** が確信

地域別特徴

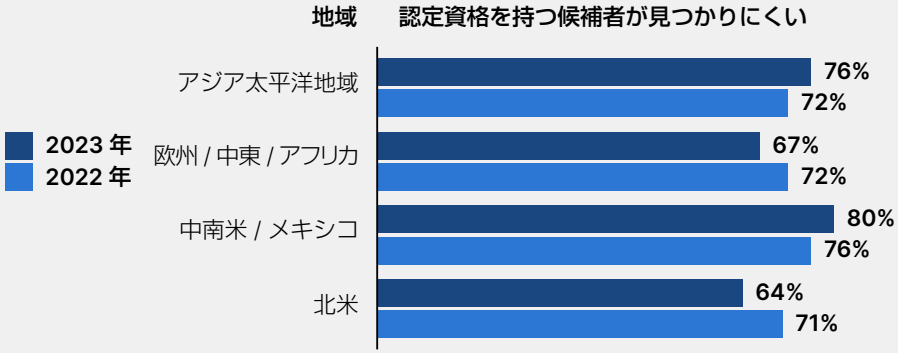
アジア太平洋地域の組織は認定資格への信頼度が高い

認定資格がスキルと知識を高めると回答した割合が最も高かったのは、アジア太平洋地域でした。



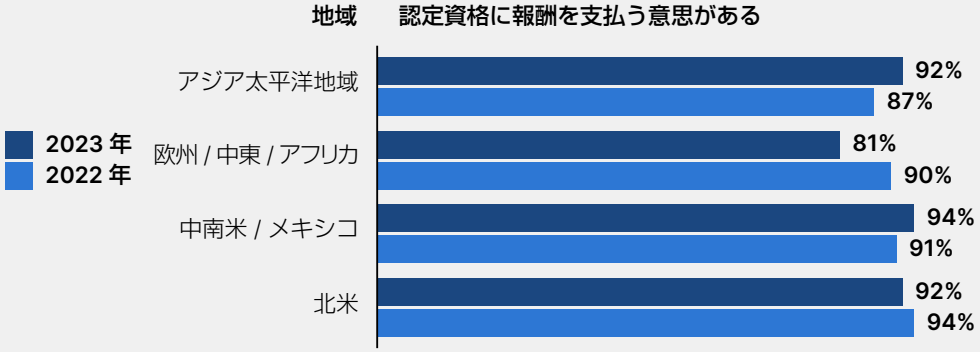
有資格のプロフェショナルが最も見つかりにくい地域は中南米 / メキシコ

企業にとって、認定資格を持つ候補者を見つけにくいのは中南米 / メキシコとアジア太平洋地域、見つけやすいのは北米と欧州 / 中東 / アフリカでした。



世界中の組織が従業員の認定資格に報酬

従業員に報酬を支払う意思がある組織はアジア太平洋地域と中南米 / メキシコで増加、北米と欧州 / 中東 / アフリカで減少しています。

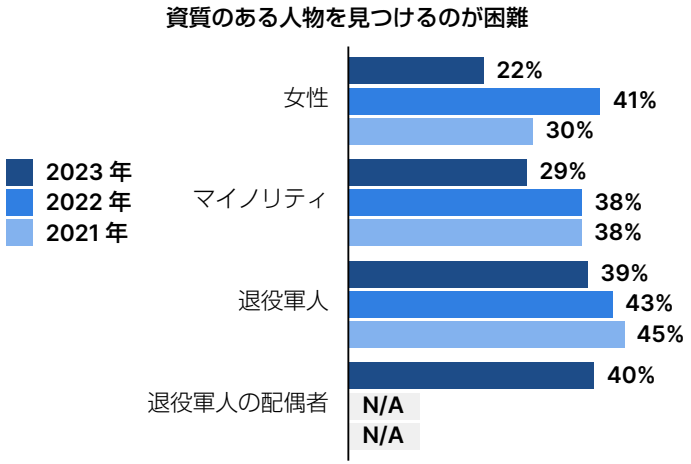


83% の組織は
今後 2 ～ 3 年間の採用に
多様性の目標を設定

実績を過小評価されている候補者の見落とし

サイバーセキュリティスキルの世界的な不足が続き、機会均等とインクルージョンが企業責任の中心に据えられる中、多くの組織が引き続きダイバーシティ採用を目標として掲げています。

大半（83%）の企業は、今後 2 ～ 3 年間のダイバーシティ採用目標を設定していると回答しました（2022 年と同じ、2021 年の 89% からやや減少）。76% は女性グループ、64% はマイノリティグループを主たる対象者としています。これは恐らく、女性やマイノリティの方が資質のある候補者を見つけやすいからと考えられます。ただし、回答者は候補者を見つける苦労はすべてのグループで減少していると答えています[1]。



それに続くグループが退役軍人とその配偶者で、それぞれ 49% と 41% です。

資質のある女性候補者を見つけやすくなった（22%）一方、積極的に女性を採用した組織は過去 2 ～ 3 年間で減少し、2022 年の 89% に対して 2023 年は 85% でした。マイノリティグループからの積極採用は比較的安定しており、退役軍人の採用は 2023 年に若干増加しました。役軍人の配偶者の採用を挙げた組織は 40% でした。

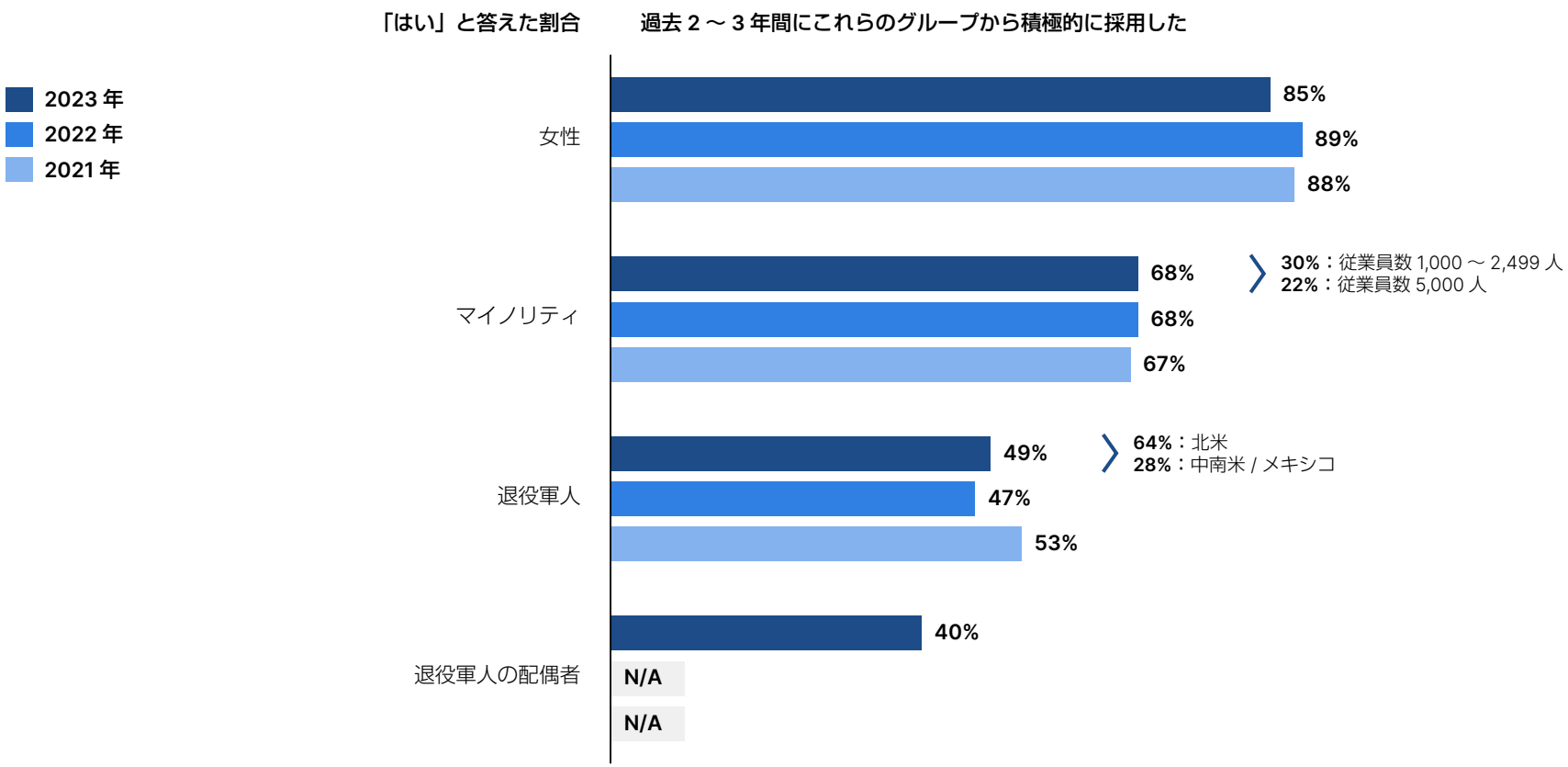
組織が必要条件の一部を変更すれば、多様性に富む従業員の募集や採用は容易になる可能性があります。

72% の回答者は、軍事訓練、専門職の資格、自己学習などの非従来的な経歴から得た資質を考慮せず、4 年制の学位が必要と答えています。組織が最小限の必要条件を変更し、実習制度や研修プログラム（80% の回答者はすでに実施）を組み合わせることで、人材プールを拡充できる可能性があります。

[1] すべてのグループに該当。ただし、過去の追跡実績がない退役軍人の配偶者を除く。

積極採用の変化

2023 年における女性の積極採用は、前年よりもやや減少しました。一方、退役軍人の採用は 2021 年より減少したものの、2023 年はわずかに増加しました。



詳細報告

対象を絞った募集プログラムによる採用人数の増加

女性を対象としたプログラムを導入する組織が増加

構造的ダイバーシティ募集計画では、引き続き女性を主たる対象者としています。

- 73% の IT 意思決定者は、女性を対象とした構造的募集計画を策定しています。
- この割合は過去 2 ～ 3 年間あまり変化がなく、2022 年は 73%、2021 年は 75% でした。

マイノリティの候補者は今なお重要なターゲット

マイノリティの候補者を対象とした募集は、2021 年から安定的に推移しています。

- 60% の組織は、マイノリティの候補者向けの構造的募集計画を実施しています。
- これは、過去数年の 59% からほとんど変わっていません。

退役軍人とその配偶者の活用は依然として進まず

退役軍人は多くの場合、規律が厳しく安全が確保された状況での勤務によって、セキュリティスキルの確固たる基礎が身についています。こうしたスキルはサイバーセキュリティに生かすことができます。

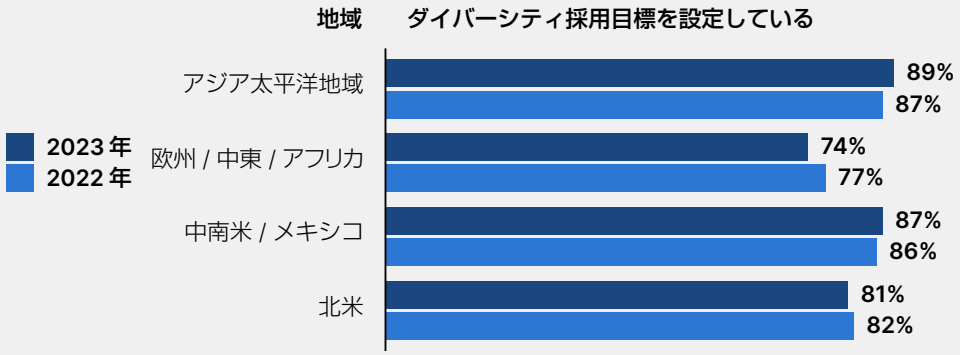
- 退役軍人を対象とした募集計画を実施している回答者は半数以下（45%）です。この割合は 2022 年（43%）から多少増加しましたが、2021 年（51%）からは減少しました。
- 退役軍人の配偶者を対象とした構造的プログラムを実施している組織はさらに少なく、36% です。

女性対象の構造的プログラムを導入する組織（73%）や女性を積極採用する組織（85%）の増加は、プログラムと成果の相関関係を示唆している

地域別特徴

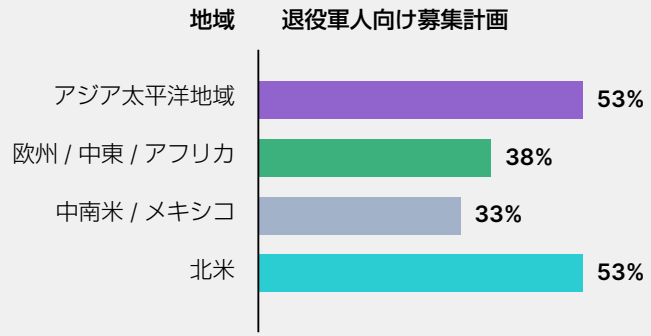
アジア太平洋地域がダイバーシティ採用目標を主導

今後 2 ～ 3 年間のダイバーシティ採用目標を設定している企業が最も多いのは、引き続きアジア太平洋地域です。最も少ない地域も欧州 / 中東 / アフリカで変わりありません。



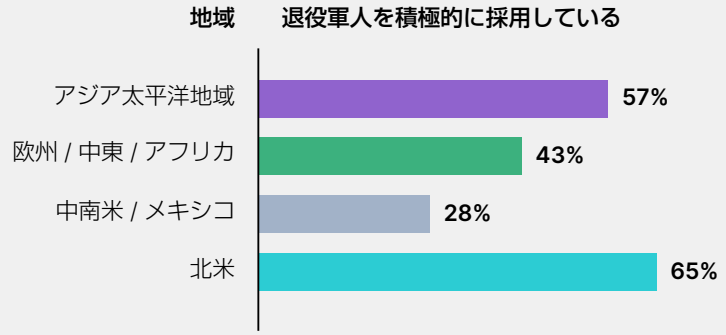
退役軍人は北米とアジア太平洋地域で需要高

退役軍人向けの構造的募集計画を実施している企業が最も多いのは、北米とアジア太平洋地域です。



北米とアジア太平洋地域で退役軍人を積極採用

以下の結果は募集計画の浸透度と密接に関係しています。



終わりに

2023 年、サイバーセキュリティは多くの組織にとって明らかに全社的な問題であり、その影響は取締役会レベルから現場の第一線にまで及んでいます。今回の調査結果は、回答者がトレーニング、意識向上、テクノロジーを組み合わせた 3 本柱のサイバーセキュリティ対策を支持していることを示しています。この対策により、現在および新たに出現する脅威に対して包括的な戦略を立てることができます。

IT およびセキュリティ専任スタッフのトレーニングと資格取得に投資し、サイバーセキュリティのベストプラクティスに対する全従業員の意識を高めることは、組織のセキュリティ態勢の強化に多いに役立ちます。新たな脅威が出現し、AI などのテクノロジーによって攻撃がより精密で巧妙かつ大規模になるにつれて、このような措置は特に重要になってくるでしょう。

適切な訓練を受け、高い知識とスキルを身につけた IT / セキュリティの専門家は、セキュリティ侵害による処罰から経営幹部や取締役を守るために不可欠です。セキュリティ意識の高いスタッフは、非常に重要な最前線の防御を可能にします。企業幹部がより大きな責任を問われるほど、サイバーセキュリティは「全員の責任」と見なされるようになるでしょう。

資格取得への投資、認定資格の継続的更新、多様で非従来型の人材プールからの採用は、スキルギャップの解消に役立ちます。組織が基本的な資格要件を厳しくし過ぎると、必要なスキルを備えた有望なサイバーセキュリティ人材を獲得する機会を狭めてしまう可能性があります。組織は募集範囲を拡大し、従来の 4 年制学位や訓練およびスキルアップの経験とは異なる実績を持つ候補者も含めることで、新たな可能性をひらくことができます。特に、認定資格やトレーニングにも報酬を支払う意思がある場合はなおさらです。

結局のところ、ほとんどの回答者が認識しているように、脅威と闘い今日の攻撃のスピードと規模に対抗するには、有能な人材に適切なサイバーセキュリティツールとスキルセットが必要だということです。スキル、知識、認定資格を高度なテクノロジーによって一つにまとめ上げることが、引き続き重要なカギとなります。

フォーティネットについて

フォーティネット（NASDAQ：FTNT）は、ネットワーク / セキュリティの融合とサイバーセキュリティの進化を、牽引し続けている企業です。あらゆる場所で、人·デバイス·データの安全を確保するというミッションのもと、お客様が必要とするすべての場所にサイバーセキュリティを提供しています。

エンタープライズでの利用に対応した 50 を超える製品群で構成される業界最大規模の統合ポートフォリオを実現し、業界最多の導入実績、特許数、認証数に支えられ、70 万を超えるお客様からの信頼を獲得しています。

脅威分析とセキュリティ研究を行う組織「FortiGuard Labs」を運営し、自社開発した最先端の機械学習や AI テクノロジーを活用することで、タイムリーかつ一貫したトップクラスの保護と共に、実用的な脅威インテリジェンスをお客様に提供しています。

また、「Fortinet Training Institute」では、誰もがサイバーセキュリティのトレーニングと新たなキャリアの機会を得られるよう、業界最大規模かつ最も広範なトレーニングプログラムを提供しています。詳しくは当社ホームページ、フォーティネットブログ、Fortinet Training Institute、FortiGuard Labs ホームページをご参照ください。

FORTINET
Training Institute

フォーティネットジャパン合同会社

〒106-0032
東京都港区六本木 7-7-7　Tri-Seven Roppongi 9 階
www.fortinet.com/jp/contact

お問い合わせ

Report-2024-Cybersecurity-Skills-Gap-202406-R1