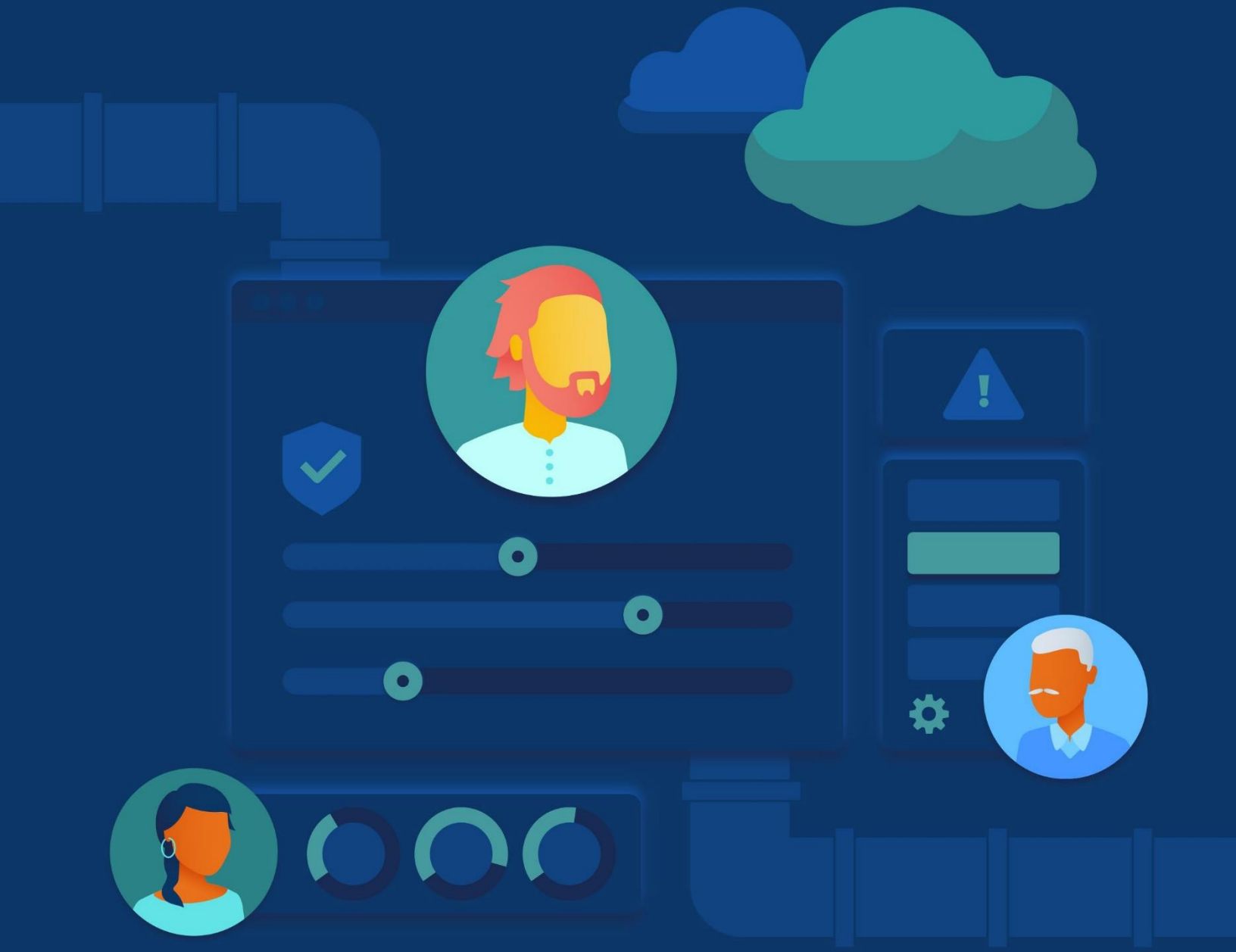
クラウド環境におけるセキュリティリスク、コンプライアンス、設定ミスの状況



CloudHealth by vmware

CSAJC cloud security alliance SM Japan Chapter

CSA cloud security alliance®

Acknowledgments

Lead Author:

Hillary Baron

Contributors:

Josh Buker
Sean Heide
Alex Kaluza
Shamun Mahmud
John Yeoh

Designers:

Stephen Lumpe
AnnMarie Ulskey

Special Thanks:

Nikhil Girdhar, *Product Marketing Leader, CloudHealth® by VMware*

Lauren van der Vaart, *Senior Content Marketing Specialist, Multi-Cloud, VMware*

日本語版提供に際しての告知及び注意事項

本書「クラウド環境におけるセキュリティリスク、コンプライアンス、設定ミスの状況」は、Cloud Security Alliance (CSA)が公開している「Cloud Thread Model in The State of Cloud Security Risk, Compliance, and Misconfigurations」の日本語訳です。本書は、CSAジャパンが、CSAの許可を得て翻訳し、公開するものです。原文と日本語版の内容に相違があった場合には、原文が優先されます。
翻訳に際しては、原文の意味および意図するところを、極力正確に日本語で表すことを心がけていますが、翻訳の正確性および原文への忠実性について、CSAジャパンは何らの保証をするものではありません。この翻訳版は予告なく変更される場合があります。以下の変更履歴(日付、バージョン、変更内容)をご確認ください。

変更履歴

日付	バージョン	変更内容
2021年12月14日	日本語版1.0	初版発行

CSAジャパン成果物の提供に際しての制限事項

日本クラウドセキュリティアライアンス(CSAジャパン)は、本書の提供に際し、以下のことをお断りし、またお願いします。以下の内容に同意いただけない場合、本書の閲覧および利用をお断りします。

1.　責任の限定

CSAジャパンおよび本書の執筆・作成・講義その他による提供に関わった主体は、本書に関して、以下のことに対する責任を負いません。また、以下のことに起因するいかなる直接・間接の損害に対しても、一切の対応、是正、支払、賠償の責めを負いません。

(1) 本書の内容の真正性、正確性、無誤謬性
(2) 本書の内容が第三者の権利に抵触しもしくは権利を侵害していないこと
(3) 本書の内容に基づいて行われた判断や行為がもたらす結果
(4) 本書で引用、参照、紹介された第三者の文献等の適切性、真正性、正確性、無誤謬性および他者権利の侵害の可能性

2.　二次譲渡の制限

本書は、利用者がもっぱら自らの用のために利用するものとし、第三者へのいかなる方法による提供も、行わないものとします。他者との共有が可能な場所に本書やそのコピーを置くこと、利用者以外のものに送付・送信・提供を行うことは禁止されます。また本書を、営利・非営利を問わず、事業活動の材料または資料として、そのまま直接利用することはお断りします。

ただし、以下の場合は本項の例外とします。

(1) 本書の一部を、著作物の利用における「引用」の形で引用すること。この場合、出典を明記してください。
(2) 本書を、企業、団体その他の組織が利用する場合は、その利用に必要な範囲内で、自組織内に限定して利用すること。
(3) CSA ジャパンの書面による許可を得て、事業活動に使用すること。この許可は、文書単位で得るものとします。
(4) 転載、再掲、複製の作成と配布等について、CSA ジャパンの書面による許可・承認を得た場合。この許可・承認は、原則として文書単位で得るものとします。

3.　本書の適切な管理

(1) 本書を入手した者は、それを適切に管理し、第三者による不正アクセス、不正利用から保護するために必要かつ適切な措置を講じるものとします。

(2) 本書を入手し利用する企業、団体その他の組織は、本書の管理責任者を定め、この確認事項を順守させるものとします。また、当該責任者は、本書の電子ファイルを適切に管理し、その複製の散逸を防ぎ、指定された利用条件を遵守する(組織内の利用者に順守させることを含む)ようにしなければなりません。

(3) 本書をダウンロードした者は、CSA ジャパンからの文書(電子メールを含む)による要求があった場合には、そのダウンロードしまたは複製した本書のファイルのすべてを消去し、削除し、再生や復元ができない状態にするものとします。この要求は理由によりまたは理由なく行われることがあり、この要求を受けた者は、それを拒否できないものとします。

(4) 本書を印刷した者は、CSA ジャパンからの文書(電子メールを含む)による要求があった場合には、その印刷物のすべてについて、シュレッダーその他の方法により、再利用不可能な形で処分するものとします。

4.　原典がある場合の制限事項等

本書がCloud Security Alliance, Inc.の著作物等の翻訳である場合には、原典に明記された制限事項、免責事項は、英語その他の言語で表記されている場合も含め、すべてここに記載の制限事項に優先して適用されます。

5.　その他

その他、本書の利用等について本書の他の場所に記載された条件、制限事項および免責事項は、すべてここに記載の制限事項と並行して順守されるべきものとします。本書およびこの制限事項に記載のないことで、本書の利用に関して疑義が生じた場合は、CSAジャパンと利用者は誠意をもって話し合いの上、解決を図るものとします。

その他本件に関するお問合せは、info@cloudsecurityalliance.jp までお願いします。

日本語版作成に際しての謝辞

「クラウド環境におけるセキュリティリスク、コンプライアンス、設定ミスの状況」は、CSAジャパン会員の有志により行われました。作業は全て、個人の無償の貢献としての私的労力提供により行われました。なお、企業会員からの参加者の貢献には、会員企業としての貢献も与っていることを付記いたします。
以下に、翻訳に参加された方々の氏名を記します。（氏名あいうえお順・敬称略）

太田　吏城
佐藤　智典
塩田　英二
神保　冬和子
鈴木　伸
満田　淳
渡邉　浩一郎　CISA,CISSP

目次

サーベイの作成と方法

クラウドセキュリティアライアンス（CSA）は、クラウドコンピューティングやIT技術におけるサイバーセキュリティを確保するためのベストプラクティスを広く推進することを使命とする非営利団体です。また、CSAは、これらの業界の様々な関係者に対して、他のあらゆるコンピューティング環境におけるセキュリティの懸念について教育することも任務としています。CSAの会員は、業界の実務家、企業、専門家団体からなる幅広い集まりです。CSAの主な目的の 1 つは、情報セキュリティの動向を評価するサーベイの実施です。これらのサーベイは、業界のさまざまな段階における情報セキュリティ技術の成熟度やセキュリティのベストプラクティスの採用率を測定するのに役立ちます。

CloudHealth®社（VMware社）は、パブリッククラウドのセキュリティに関する業界の知識を深めるためのサーベイと、サーベイ結果をまとめた本レポートの作成をCSAに委託しました。CloudHealth社はこのプロジェクトに資金を提供し、クラウドセキュリティに対応したサーベイ項目の開発にCSAと共同で参加し、この取り組みを進めました。このサーベイは、CSAによって2021年5月から2021年6月までオンラインで実施され、さまざまな規模と場所の組織のITおよびセキュリティの専門家から1090件の回答を得ました。データ分析はCSAのリサーチチームが行いました。

調査の目的

本サーベイの目的は、設定ミスによるパブリッククラウドのセキュリティとコンプライアンスリスクを軽減するための組織の準備状況を評価することです。主な調査テーマは以下のとおりです：

- 重大リスクやセキュリティツールの使用状況など、クラウドセキュリティプログラムの現状
- 構成ミスの脆弱性を軽減するために組織が直面するクラウドセキュリティポスチャ管理（CSPM）の課題
- 組織の準備状況、成功のためのKPI、クラウドセキュリティポスチャ管理のさまざまな側面を担当するチーム

エグゼクティブサマリー

パブリッククラウドを利用する企業にとって、クラウドの設定ミスは常に最大の懸念事項です。このようなミスは、データの漏洩、リソースの削除や変更、サービスの中断など、ビジネスの運営に大きな影響を与えます。今回の調査は、設定ミスによる情報漏えいが大きな話題となっていることから、クラウドセキュリティプログラムの現状、セキュリティリスクを軽減するために利用しているツール、企業のクラウドセキュリティ対策、セキュリティリスクを軽減する上で企業が直面している障害などについて理解を深めるために実施しました。

主要な所見 1:

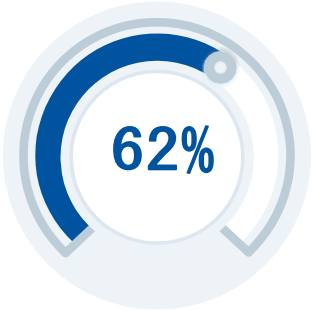
セキュリティチームを悩ませる知識と専門性の欠如

情報セキュリティ業界では、知識やノウハウの不足が問題となっています。目新しいことではありませんが、その知識や専門性の欠如が一貫して指摘されています：

- クラウドセキュリティ全般における主な障壁（59%）
- 設定ミスの主な原因（62%）
- 設定ミスを予防的に防止または修正するための障壁（59%）
- 自動修復を実施する際の主な障壁（56%）

この調査結果は、知識不足がセキュリティチームに与えるトリクルダウン効果を浮き彫りにしています。これは、効果的なクラウドセキュリティ対策を実施するための一般的な障壁として始まります。これは、データ漏洩の主な原因である設定ミスにつながります。一方で、このような知識やスキルの不足を補うことができる自動修復などのソリューションをセキュリティチームが導入することを妨げています。

クラウドセキュリティ全般における主な障壁



設定ミスの主な原因

設定ミスを予防的に防止または修正するための障壁

自動修復を実施する際の主な障壁

主要な所見 2:

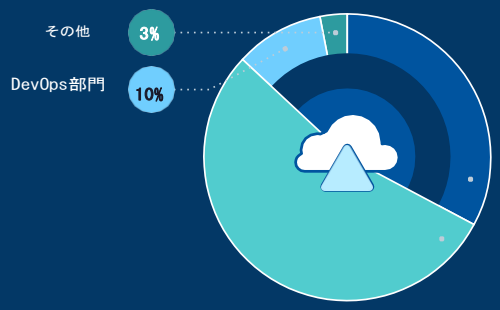
クラウドの設定ミスを減らすために、情報セキュリティとIT運用部門が責任を負う

毎年、設定ミスによるデータ流出が話題になり、多くの企業にとって最大の懸念となっています。
企業が設定ミスの管理に苦慮している理由の一つとして、IT運用部門や情報セキュリティ部門が、潜在的な設定ミスの検出、監視、追跡(**情報セキュリティ 54%**, **IT 運用 33%**)、およびこれらの設定ミスの修正(**情報セキュリティ 36%**, **IT 運用 34%**) に対する責任を負っていることが挙げられます。これらのミスを直接修正するのに適した立場にあるDevOpsチームやアプリケーションエンジニアリングチームに責任を分散しておらず、このようなミスを偶然に引き起こしている可能性があります。
このため、企業は、設定ミスのリスクをより効果的に管理するために、修正の責任をDevOpsチームやアプリケーションエンジニアリングチームに委ねることが重要です。
また、設定ミスが原因でセキュリティインシデントが発生した場合の主な理由として、「可視性の欠如」(68%)が挙げられています。組織にとっては、3つの主要な機能を提供するツールを優先することが同様に重要です:

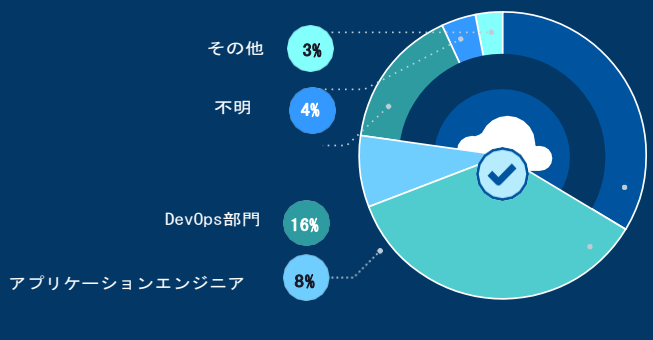
- 可視性の向上
- 効果的なリスクガバナンス
- 自動化

これらの機能は、設定ミスを担当する部門がどこであれ、組織が迅速に設定ミスを特定して修正する能力を向上させるのに役立ちます。

あなたの組織でクラウドの設定ミスを検出、追跡、報告をする責任を負っている部門はどこですか



あなたの組織でクラウドの設定ミスを確実に修正する責任を負っている部門はどこですか



主要な所見 3:

DevSecOpsによるセキュリティのアプローチが行き届いていない

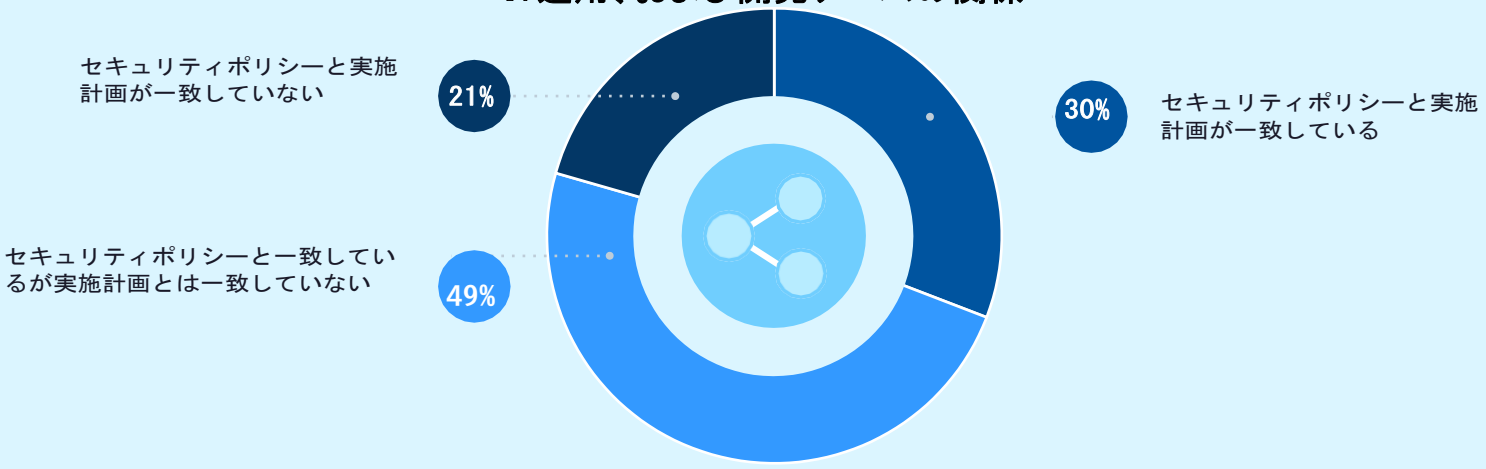
セキュリティポリシーやその他の施策について部門間の調整が困難

セキュリティ業界では、「DevSecOps」や「セキュリティのシフトレフト」などのトピックがますます注目を集めています。これらの戦略は、よりセキュリティを強化し、より安全で、よりレジリエンスなアプリケーションを実現するものですが、多くの組織ではこれらのアプローチの導入に苦労しています。セキュリティポリシーとその施行について、部門間で合意を得ることさえ困難であり、この点で成功している組織は3分の1以下です。

このように部門間の連携が取れていないのは、文化の違い、つまりマネージャー間の優先順位の違いが原因である可能性があります。一般的に、この問題はマネージャーから始まり、チームに広がっていきます。連携不足のもう一つの原因の可能性は、先の主要調査結果で指摘した知識不足です。もし各部門がDevSecOpsの戦略やベストプラクティスについて十分な知識を持っていなければ、それらの導入を開始したり、重要な問題について意見を一致させたりすることは非常に困難になります。

また、約70%の企業がセキュリティポリシーや実施に関する部門間の調整に苦労しているにもかかわらず、これをセキュリティ問題解決の主な障壁と認識しているのは39%に過ぎないことも注目に値します。つまり、DevSecOps モデルやシフトレフトモデルへの移行を妨げているのは、より根本的な問題であると考えられます。

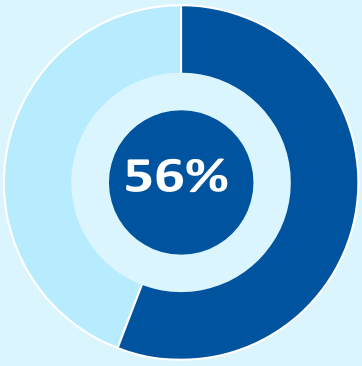
セキュリティポリシーと実施に関する、セキュリティ、IT運用、および開発チームの関係



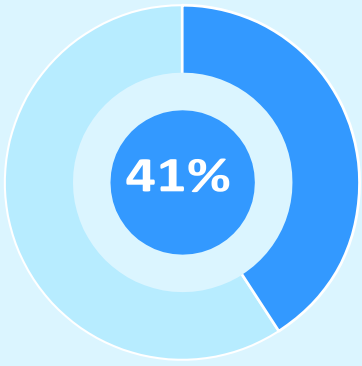
プロアクティブなセキュリティの実現には、セキュリティポリシーと実施に関する部門間の調整が重要

セキュリティポリシーと実施戦略に関して部門間の整合性が取れており、DevSecOps のアプローチに移行している組織は、設定ミスに対処する体制が整っています。これらの組織では、設定ミスが発生してから1日以内に検出する割合が高くなっています（**その通り: 56%**、**一部その通り: 41%**、**そうではない: 31%**）。また、設定ミスを検出してから 1 日以内にそのエラーを修正できる可能性も高くなっています(**その通り: 51%**、**一部その通り: 24%**、**そうではない: 19%**)。設定ミスは、データ漏洩の主要な原因の一つであるため、ミスを検出して修正するまでの時間が短ければ短いほど、データ漏洩を防ぐことができます。
このようなエラーが発生すればするほど、組織全体のセキュリティが向上します。組織が設定ミスに対処するだけでなく、データ漏洩やその他の重大なセキュリティインシデントのリスクを低減するためには、このような連携とDevSecOpsのアプローチへの動きが鍵となることは明らかです。

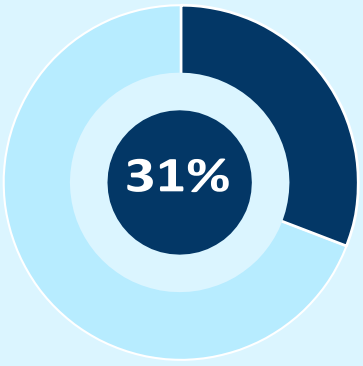
設定ミスを1日以内に発見できるか



セキュリティポリシーと実施についての整合性がある

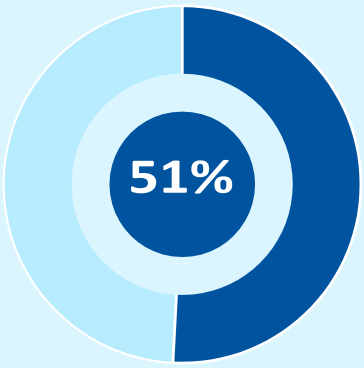


セキュリティポリシーは一致しているが、実施されていない

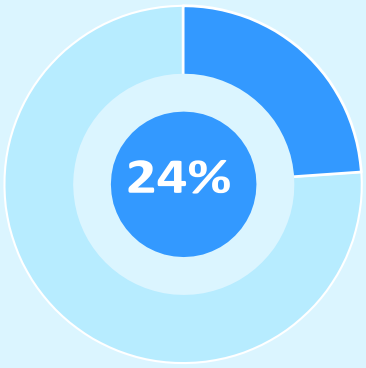


セキュリティポリシーや実施が一致していない

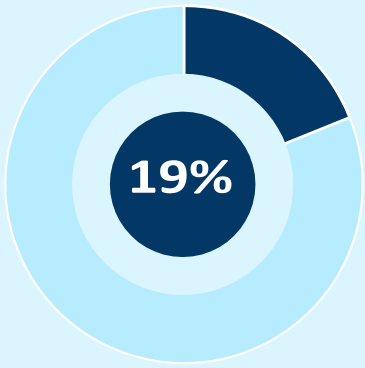
設定ミスを1日以内に修復できるか



セキュリティポリシーと実施についての整合性がある



セキュリティポリシーは一致しているが、実施されていない

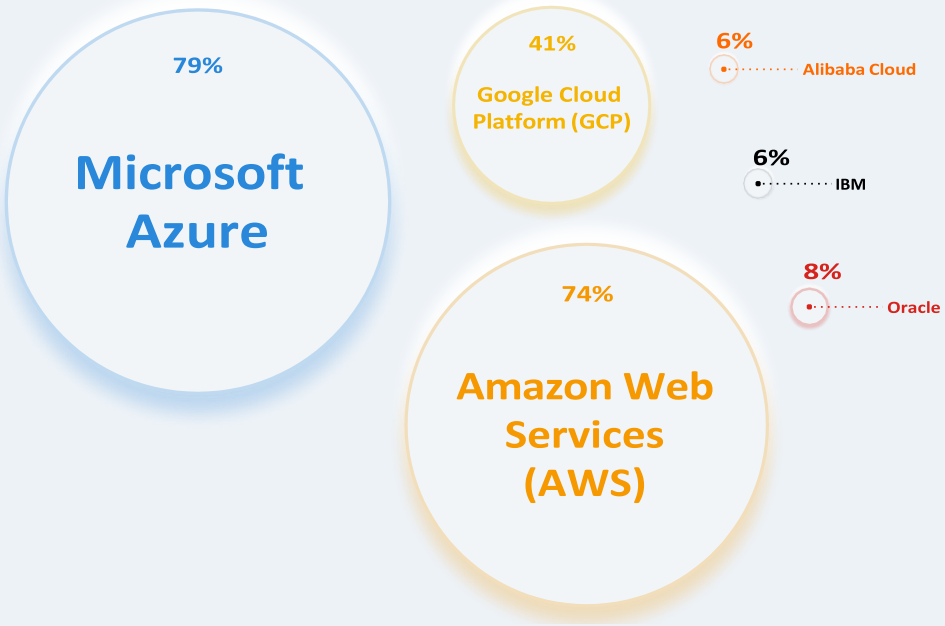


セキュリティポリシーや実施が一致していない

クラウドセキュリティプログラムの現状

利用されているパブリッククラウドプロバイダ

パブリッククラウド市場では、独占的なプラットフォームはありませんが、Amazon Web Services（AWS）、Microsoft Azure、Google Cloud Platform（GCP）が引き続き主要なパブリッククラウドプロバイダとして利用されています。今回の調査では、**回答者の74%がAWS、79%がAzureを、41%がGCPを利用しています**。

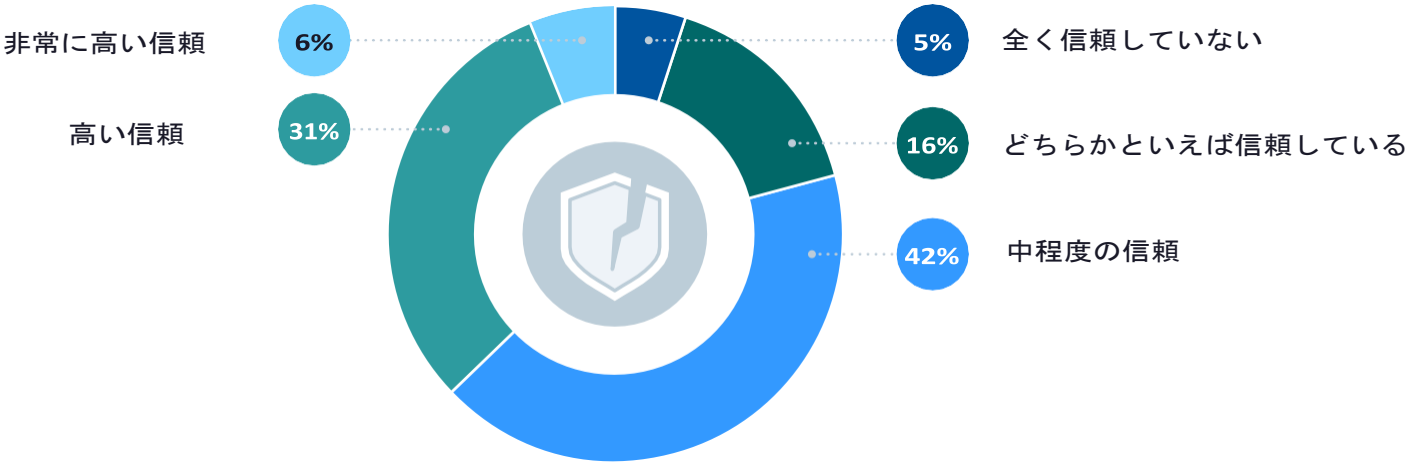


パブリッククラウドの年間予算

パブリッククラウドにかける予算は、回答者によって大きく異なりました。しかし、**「$0-$250,000」が22%**、**「$500,001-$1,500,000」が15%** 、**「$250,001-$500,000」が13%**と150万ドル以下の回答が上位3位を占めました。また「unsure（わからない）」（16%）という回答も目立ちました。

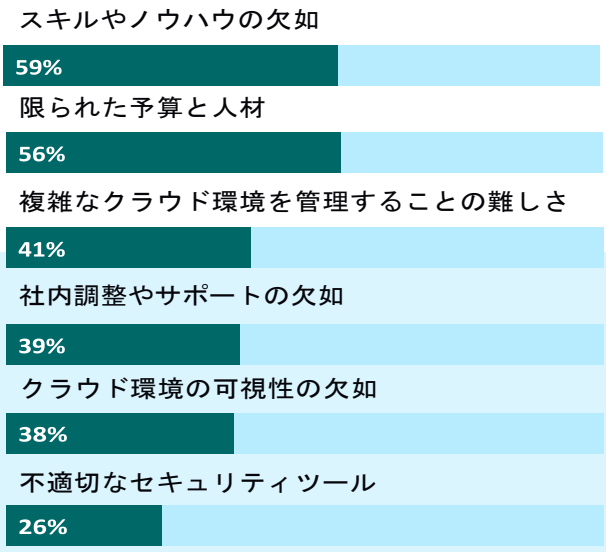
クラウドセキュリティ侵害に対する全般的な信頼度

回答者の組織のセキュリティプログラムに対する信頼度を評価するため、回答者にクラウドのセキュリティ侵害に対する組織の防御能力の全般的な信頼度を尋ねました。ほとんどの回答者は、**「中程度の信頼」（42%）**または**「高い信頼」（31%）**と回答しました。



クラウドの脆弱性と脅威に対する防御能力への信頼度

各カテゴリーにおける脅威や脆弱性に対する防御能力について、平均的に回答者は自組織の能力に「おおむね信頼している」と回答しています。カテゴリー間での回答に大きな差はなく、最も信頼感が高かった「コンプライアンスと規制」と「ネットワーク」は、最も評価の低かった「設定ミス」をわずかに上回った程度にとどまりました。



セキュリティへの懸念解消に立ちはだかる障壁

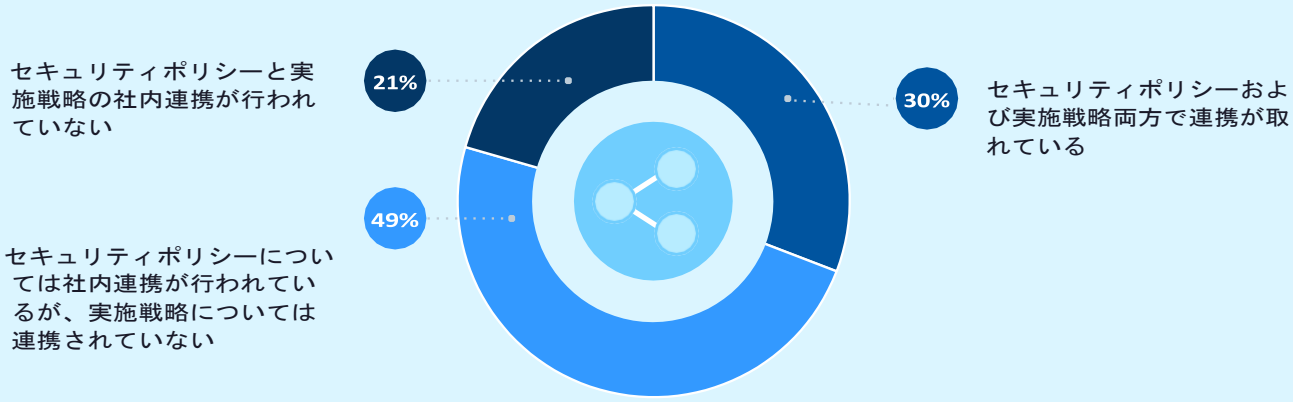
セキュリティに関する問題を解決するための主な障壁は、**「スキルやノウハウの不足」（59%）**と**「限られた予算と人材」（56%）**というおなじみの問題でした。この2つの問題は、以前から業界を悩ませており、他の選択肢と密接に関連しています。このことは、予算、スタッフ、専門知識の問題が、他の重要な問題、例えば「可視性の欠如」や「不適切なセキュリティツール」など、他の重要な問題が見えなくなっている可能性があります。

セキュリティポリシーと実施に関する部門間の連携

セキュリティ業界では、「DevSecOps」や「シフトレフト」という言葉がよく使われます。しかし、多くの組織では、これらのコンセプトを実行に移すことができていないようです。社内のチームが、セキュリティポリシーと実施戦略の両方について連携していると回答したのは、わずか31%です。このように部門間の連携が取れていないのは、文化の違い、すなわち優先順位の違いによるものと考えられます。また、前の質問で指摘したように、知識が不足していることも考えられます。

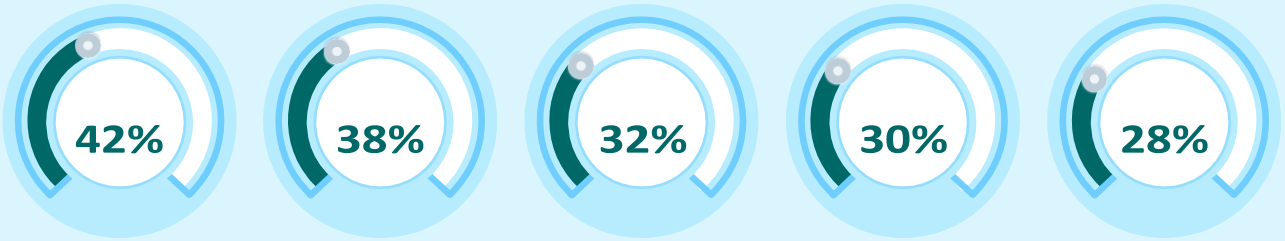
また、約70%の企業が、セキュリティポリシーや実施に関する部門間の調整に苦労しているにもかかわらず、これをセキュリティ問題解決の主な障壁と認識しているのは39%にとどまっていることも注目に値します。

さらに、セキュリティポリシーや実施ポリシーに関する部門間の調整がうまくいっているという回答者は、セキュリティ侵害に対する防御能力に「非常に自信がある」または「自信がある」と回答する傾向にあります（「非常に自信がある」：完全な調整が15%、部分的な調整が2%、調整なしが1%、「自信がある」：完全な調整が49%、部分的な調整が27%、調整なしが16%）。明らかに、社内の連携は、クラウドのセキュリティポスチャを改善しようとしている企業にとって、重要な決定要因であり、基本的な要件であることがわかります。



セキュリティとコンプライアンスのポスチャの評価

セキュリティとコンプライアンスのポスチャを測るために使用している指標は、組織によって異なります。回答者には、自社で使用している指標のうち、上位3つを選択してもらいました。最も多く選択された回答は、**「高リスクの設定ミスまたは違反の未解決率」(42%)、「失敗したセキュリティおよびコンプライアンス管理策の数」(38%)、「設定ミスまたはセキュリティおよびコンプライアンス違反を解決するまでの平均時間」(32%)でした。**



高リスクの設定ミスまたは違反の未解決率

失敗したセキュリティおよびコンプライアンス管理策の数

設定ミスやセキュリティ・コンプライアンス違反を解決するまでの平均時間

設定ミスやセキュリティ・コンプライアンス違反を検知するまでの平均時間

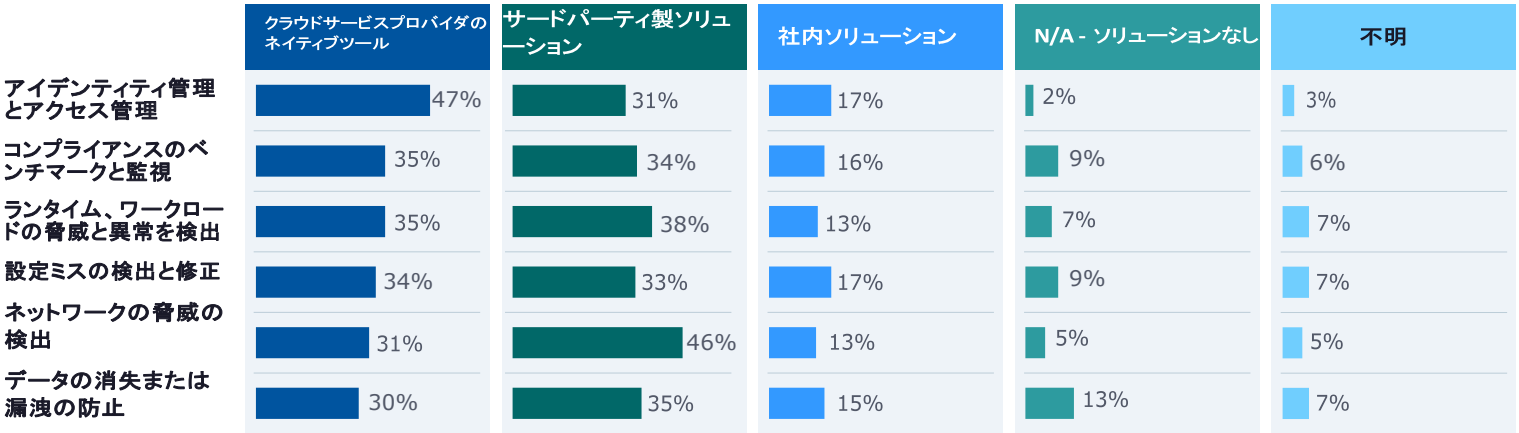
セキュリティ・コンプライアンス管理の管理対象となるクラウドインベントリの割合

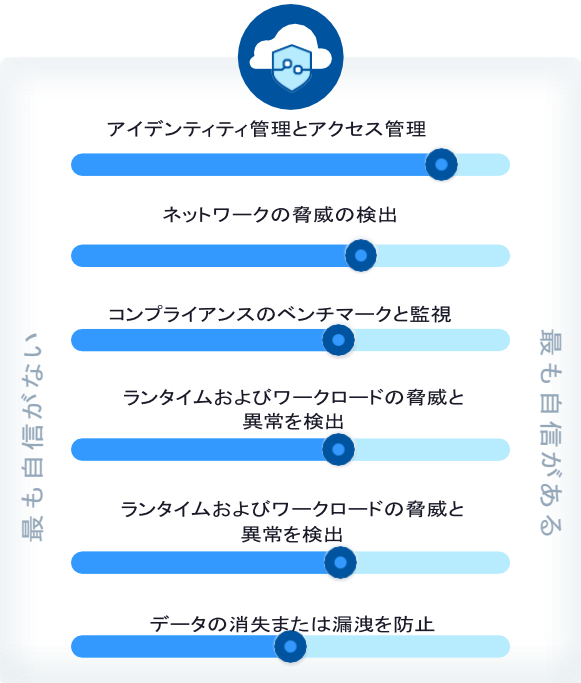
使用するクラウドセキュリティツール

クラウドセキュリティに使用されるソリューション

一般に、クラウドサービスプロバイダのネイティブツールとサードパーティのソリューションを使用している組織は、比較的均等に分かれています。しかし、クラウドセキュリティのいくつかのカテゴリーが明らかに勝っていました。クラウドサービスプロバイダのネイティブなツールは、**「アイデンティティとアクセス管理」(47%)**のための好ましいソリューションであり、一方、サードパーティのソリューションは、**「ネットワークの脅威を検出する」(46%)**と**「データ漏洩を防ぐ」(35%)**のために好ましいソリューションであります。

特に注目すべきパターンは、データ漏洩防止ツール（DLP）を使用していない組織の割合(13%)で、これは他のどのカテゴリーよりもはるかに高かったです。これは、これらのタイプのソリューションを実装することが難しいことを反映している可能性があります。

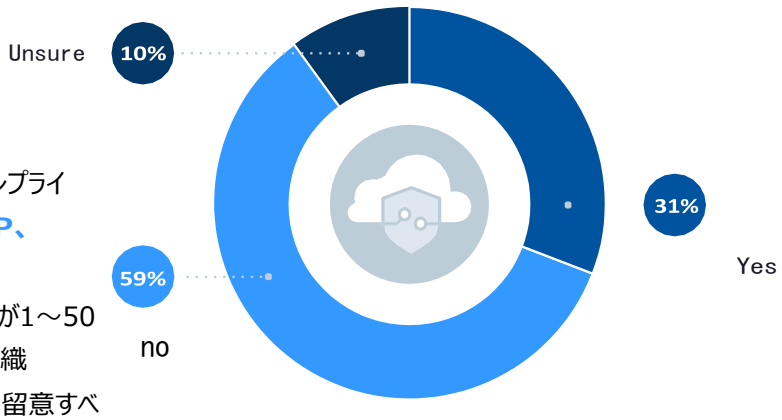




クラウドウドサービスプロバイダのセキュリティソリューションに対する満足度

回答者は平均して、主なパブリッククラウドサービスプロバイダのセキュリティソリューションに「中程度に満足している」と回答しています。各カテゴリーの満足度にはわずかなばらつきがありました。「IDおよびアクセス管理」など、平均満足度が最も高かった分野は、「データの損失または漏洩を防ぐ」という最も低い評価よりもわずかに高いだけでした。

マネージドサービスプロバイダの利用



ほとんどの組織は、パブリッククラウド環境のセキュリティとコンプライアンスを管理するためにマネージドサービスプロバイダ(**MSP、59%**)を使用していません。**わずか31%がMSPを使用しています。**従業員数が1～50人の小規模企業(72%)は、従業員数が50人以上の組織(57%)よりもMSPを使用しない可能性が高かったことにも留意すべきです。

クラウドセキュリティポスチャマネジメント（CSPM）

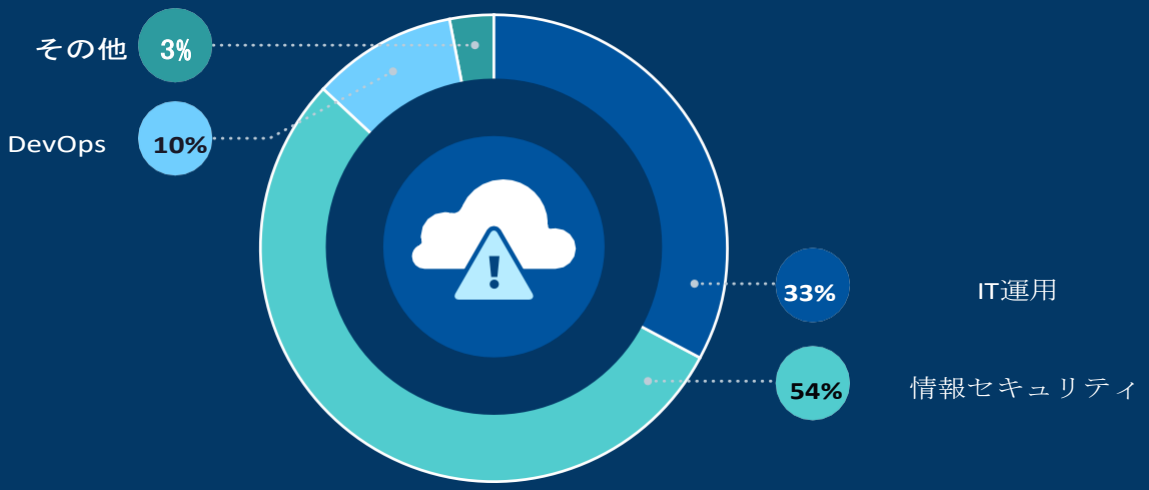
設定ミスの特定

設定ミスの検出、追跡、報告を担当するチーム

クラウドの設定ミスを検出、追跡、報告する主な担当チームは、**情報セキュリティチームであることが最も多く（54%）**、2番目に多かった回答は「ITオペレーション」**（33%）**でした。

興味深いのは、通常、設定ミスの発生源であり、設定ミスが発生したことに気づく可能性が高いDevOpsチームが、クラウドの設定ミスの検出、追跡、報告を担当するグループとして認識されていないことでした。このことは、部門間の連携と可視性を向上させるために、DevSecOpsのアプローチに移行することの重要性を示しています。その結果、最終的には設定ミスの迅速な検出と修正が可能になります。

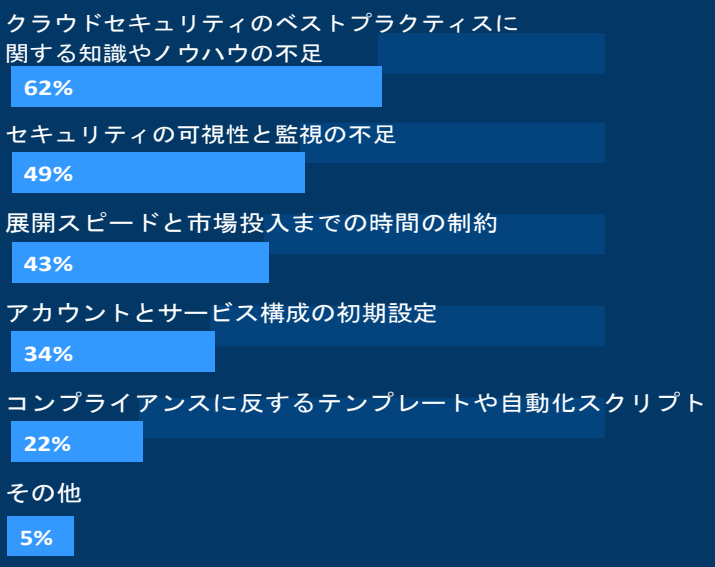
同様に重要なのは、これらの部門を組織全体で有効にするための適切なツールを組織が持つことです。特に、効果的なリスクガバナンスを可能にするツールがあれば、組織はリスクとコンプライアンスをより適切に特定し、管理することができます。また、設定ミスを迅速に特定して修正するためには、自動化が重要です。そのためには、組織のアーキテクチャをクラウドに向けて最新化する必要があります。



クラウド設定ミスの原因

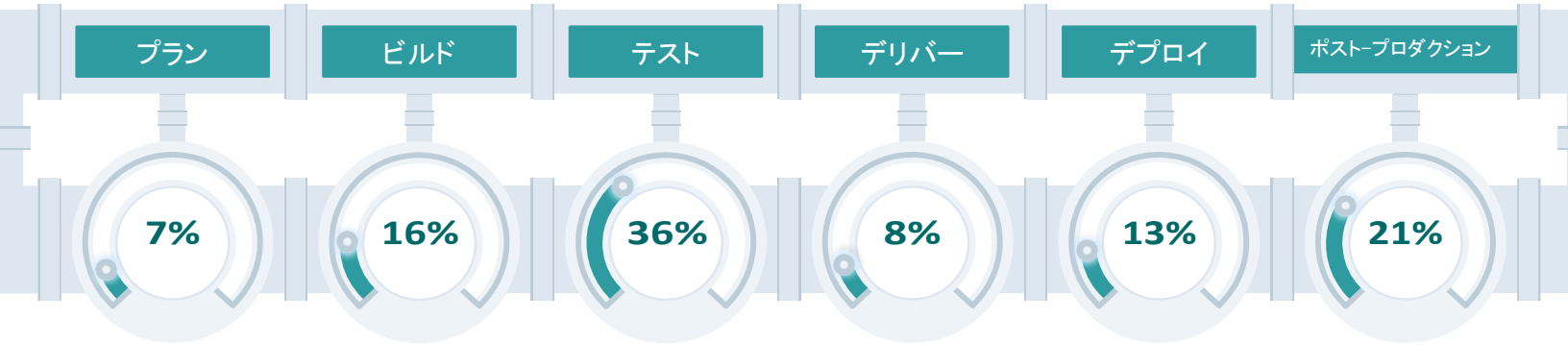
企業における設定ミスの主な原因は、「クラウドセキュリティのベストプラクティスに関する知識やノウハウの不足」（62%）でした。これは 先に述べたように、セキュリティ上の大きな障壁となっていることから、当然のことと言えるでしょう。さらに意外だったのは、2番目に多かった回答である「セキュリティの可視性と監視の不足」（49%）でした。

「セキュリティの可視性と監視の欠如」（49%）という回答が2番目に多かったのは、少し意外でした。なぜなら、この調査では、セキュリティに関する懸念を解決するための主要な障壁として可視性が挙げられていなかったからです。このことは、組織が可視性に関する課題の解決を優先していないことを示していると考えられます。その結果、可視性が設定ミスの主な原因となっていることを示していると考えられます。



設定ミスが発見されるパイプラインデリバリーフェーズ

クラウドの設定ミスが検出されるパイプラインフェーズで最も多いのは、「テスト」段階（36%）と「ポストプロダクション」段階（21%）です。つまり、ほとんどの設定ミスは導入前に検出されており（67%）、少なくともいくつかの方法で企業は "シフトレフト "することができていたと考えられます。

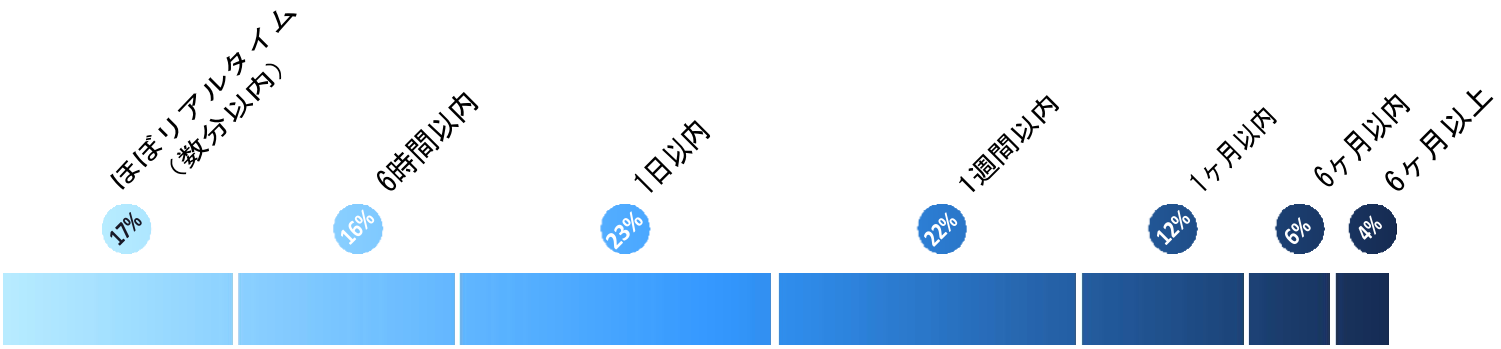


設定ミスを検知するまでの時間

クラウドの設定ミスを発見するまでの時間は、組織によって大きく異なります。最も多いのは、1日以内（23%）または1週間以内（22%）に発見していることです。しかし、懸念すべきは、22%の企業が、設定ミスの解決はおろか、設定ミスを発見するのにも1週間以上かかっていることです。

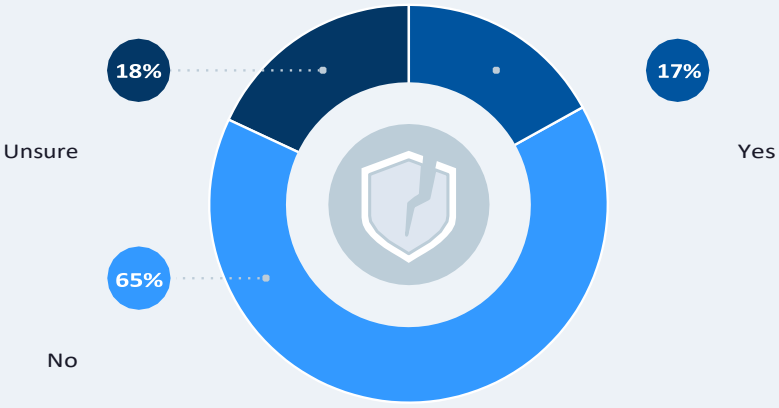
また、ポリシーとその実施に関する部門間の連携を報告した組織では、エラーが発生してから1日以内に設定ミスを検出する可能性が高かったことも重要です（完全連携：56%、部分連携：41%、連携なし：31%）。

.

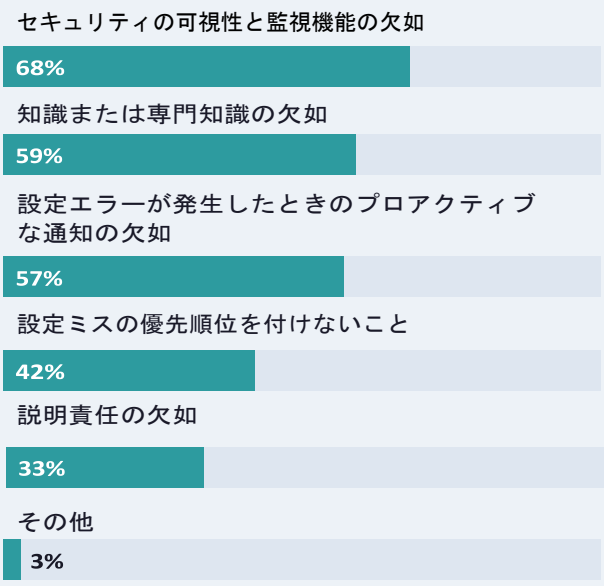


設定ミスによる侵害とインシデント

過去一年間に発生した設定ミスによるクラウドセキュリティインシデントまたは侵害



ほとんどの企業は、過去1年間にパブリッククラウドのセキュリティインシデントや侵害を経験していないと回答しました（65%）。約17%がそのようなインシデントを経験したことがあると回答し、18%はわからないと回答しました。この調査の回答者は、組織のクラウドセキュリティ対策に直接関与する職務に就いていることを考えると、セキュリティインシデントや侵害が発生したかどうかわからない、という回答率が高いのは気になります。



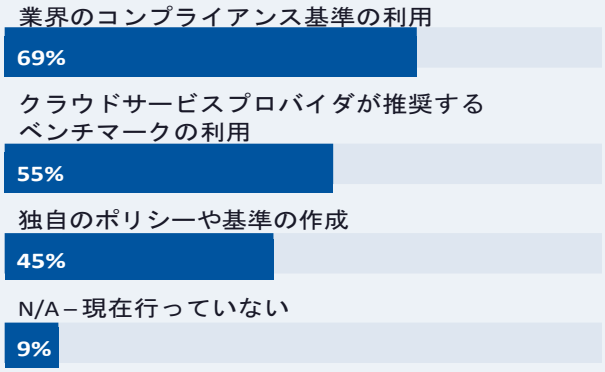
クラウドの設定ミスの修正を妨げる要因

クラウドセキュリティインシデントまたは侵害が発生した17%のうち、原因を積極的に防止または修正するための最も一般的な障壁は、「セキュリティの可視性および監視機能の欠如」（68%）であり、次いで「知識または専門知識の欠如」（59%）でした。繰り返しになりますが、知識と可視性が重要な障壁となっています。

ガバナンスとコンプライアンス

クラウドの設定ミスを管理するためのセキュリティおよびコンプライアンス基準の設計

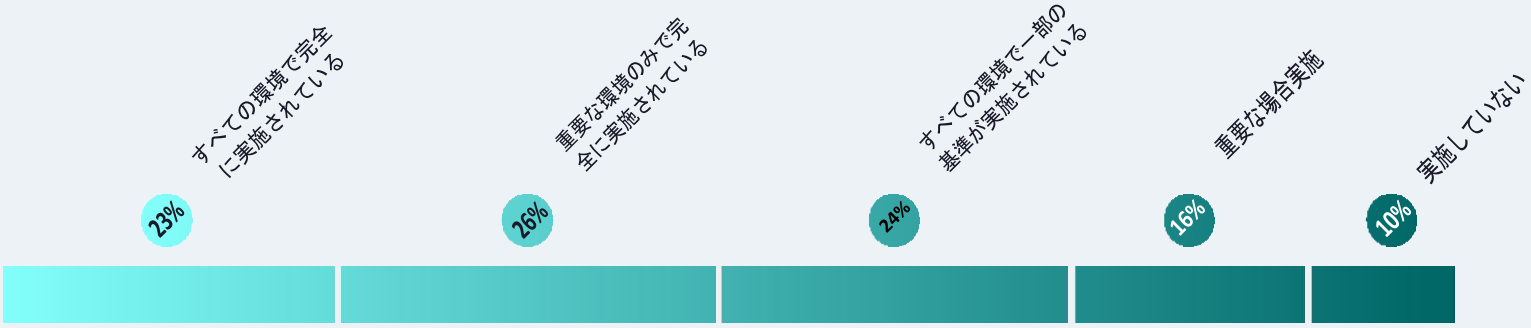
企業は主に、「業界のコンプライアンス基準」（69%）、「クラウドサービスプロバイダが推奨するベンチマーク」（55%）、「独自のポリシーや基準」（45%）を利用しています。この結果、セキュリティ・コンプライアンス基準の設計を現在行っていないと回答したのは、わずか9%でした。



チームや組織を超えた標準化の実施

セキュリティおよびコンプライアンス基準の実施レベルは、組織によって異なります。「すべての環境で完全に実施されている」（23%）、「重要な環境のみで完全に実施されている」（26%）、「すべての環境で一部の基準が実施されている」（24%）と回答した企業はほぼ同数であった。特に興味深いのは、70%の企業が、セキュリティポリシーやその実施に関する部門間の調整に苦労していると回答していることです。

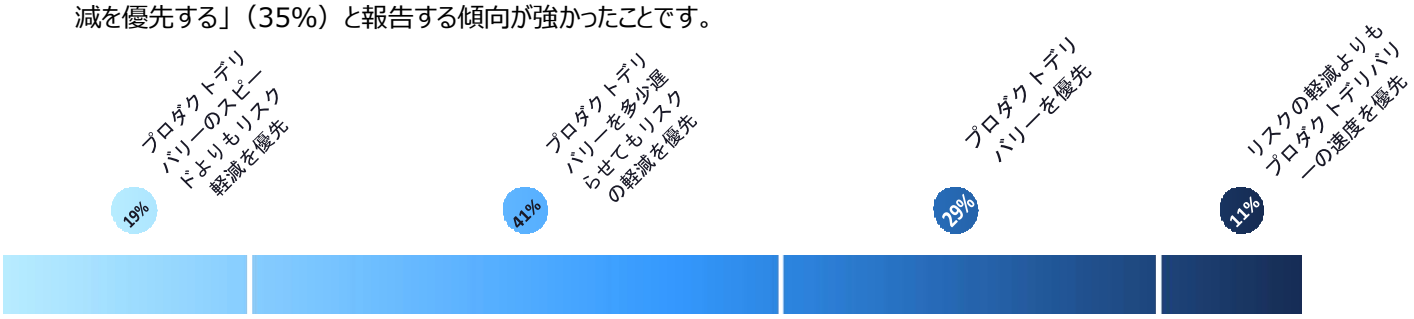
ポリシーとその実施に関して部門間で連携している組織では、「すべての環境で完全に実施されている」と回答した割合が44%であり、ポリシーについては連携しているが実施はしていない（17%）、どちらについても連携していない（7%）と比較して高かったことも注目すべき点です。



セキュリティとプロジェクト遂行のバランス

調査対象となった組織は、プロダクトデリバリーのスピードが多少遅れても、リスクの軽減を優先する傾向があります（41%）。29%は、リスク軽減を多少遅らせても、プロダクトデリバリーのスピードを優先しています。今回の調査では、情報セキュリティ専門家が多数回答しているため、これらの回答に偏りがないことを確認するために、彼らの回答を省略してデータを分析しました。その結果、有意な差は見られませんでした。

もう一つの注目すべき結果は、ポリシーとその実施に関して部門間で連携している組織は、ポリシーについては連携しているが実施はしていない（12%）、どちらも連携していない（12%）と比較して、「プロダクトデリバリーよりもリスクの軽減を優先する」（35%）と報告する傾向が強かったことです。



設定ミスの解決

設定ミスの修正を担当するグループ

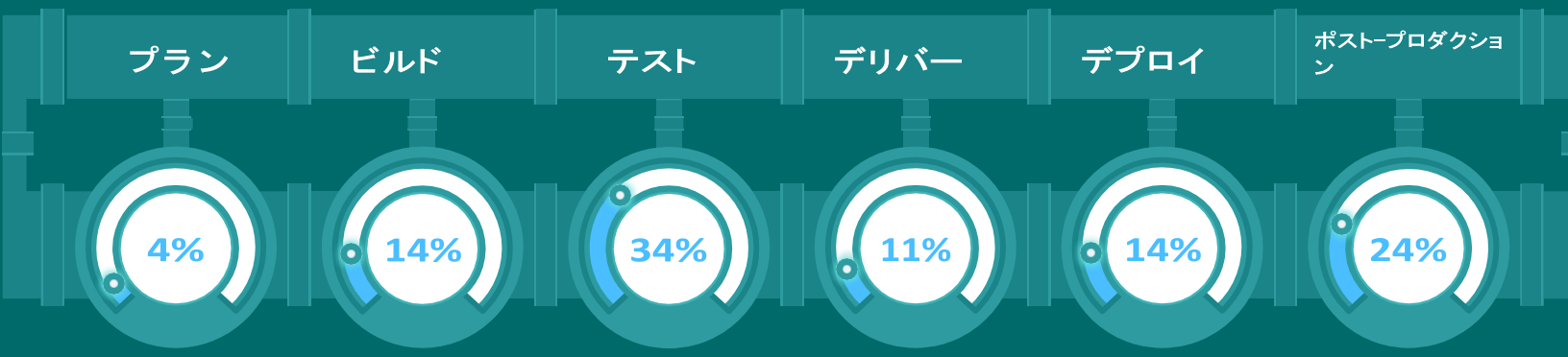
前に記述しているように、クラウドの構成ミスの検出、追跡、および報告を担当する主要なグループは情報セキュリティ（54%）であり、IT運用（33%）がそれに続きます。 設定ミスの解決に関しては、情報セキュリティとIT運用が依然として2つの主要な責任グループです。 ただし、責任の分担ははるかに均等に分割されているように見えます。情報セキュリティを報告している組織の36%が主に責任を負い、IT運用を報告している組織の34%が主に責任を負っています。

このようなミスを引き起こし、これらのエラーを直接修正するためのより良い立場にあるDevOpsまたはアプリケーションエンジニアチームではなく、IT運用と情報セキュリティが責任を負っているのは興味深いことです。これは、これらの部門間の調整の重要性をもう一度強調しています。組織がこの調整を行い、DevSecOpsアプローチに移行できれば、他の部門の活動をより明確に把握できるようになり、組織は協力して、構成の誤りや発生するその他のエラーに迅速に対処できます。

設定ミスが修正されるパイプライン配信段階

クラウド構成エラーが修正される配信パイプラインの最も一般的な段階は、「テスト」フェーズ（34%）と「ポストプロダクション」フェーズ（24%）です。これは、ほとんどの構成エラーが配備前に修正されていることを意味し（63%）、少なくともいくつかの方法で組織が「シフトレフト」できていることを再度示唆しいています。

これらの調査結果は、クラウド構成エラーが検出された配信パイプラインの段階とほぼ同じです。これについては、前に説明しました（テスト、36%、ポストプロダクション、21%、展開前の修正、67%）。



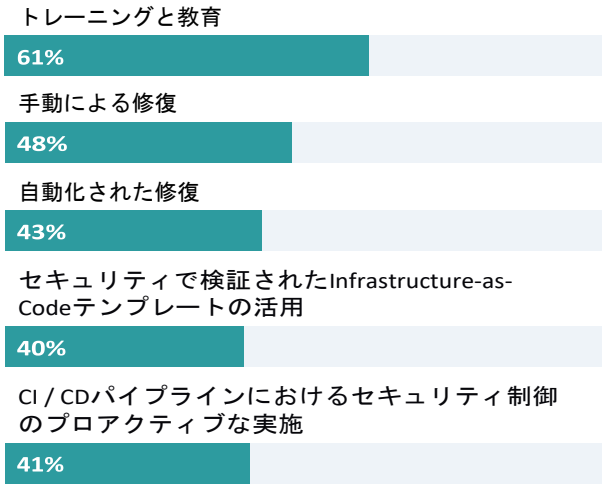
設定ミスを修正する時間の長さ

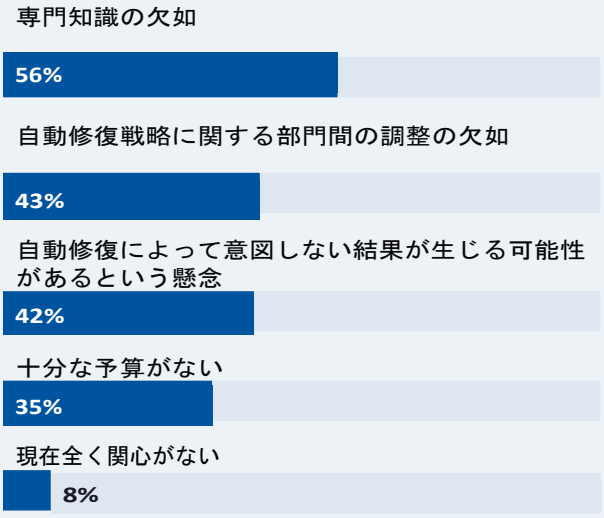
ほとんどの組織は、同じ週（32%）または同じ日（28%）のうちにこれらのクラウド構成の誤りを修正しています。ただし、組織の約30%においては、これらの設定ミスを修正するのに1週間以上かかっています。

構成の誤りを検出する時間の長さに関する同様の質問では、78%の組織が1週間以内にエラーを検出できたことがわかりました。同様の傾向は、構成エラーを修正する時間の長さでも見られ、69%が1週間以内に修正しました。もう1つの注目すべき発見は、ポリシーとその実施に関する部門間の調整を報告した組織も、構成の誤りを検出してから1日以内にそのエラーを修正する可能性が高いことです（完全な調整 -51%、部分的な調整 -24%、調整していない -19%）。

セキュリティまたはコンプライアンスの設定ミスの解決を改善する方法

組織がクラウド環境でのセキュリティやコンプライアンスの設定ミスの解決を改善するために使用する最も一般的な方法は、「トレーニングと教育」でした。知識の欠如がセキュリティの主要な障壁として繰り返し示されているため、これは驚くべきことではありません。2番目と3番目に多い回答は、「手動による修復」（48%）と「自動化された修復」（43%）でした。自動化が上位から3番目の方法になりましたが、前の質問で組織が設定ミスを修正するのにかかる時間について尋ねたときに一般的に選択された回答ではなかったため、多くの組織がまだ完全に自動修復を実装していないことは明らかです。





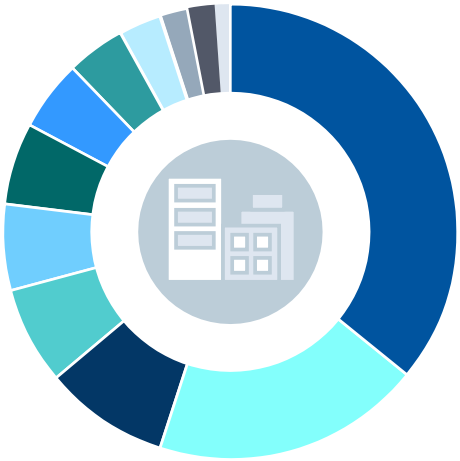
自動修復を使用する際の障壁

自動修復を利用していない人にとって、このソリューションを使用しない最も一般的な理由は、専門知識の欠如（56%）でした。2番目に一般的な理由は、自動修復戦略に関する部門間の調整の欠如でした（43%）。組織の70%が、セキュリティポリシーやポリシーの実施に関して部門間の調整を行うのに苦労しているため、これも驚くべきことではありません。3つ目の理由は、自動修復によって意図しない結果が生じる可能性があるという懸念があったことです（42%）。これは、専門知識と知識の欠如の問題に結びつく可能性があります。チームがテクノロジを適切に利用する方法を知らない場合、意図しない結果に遭遇する可能性が非常に高くなります。

回答者の統計情報

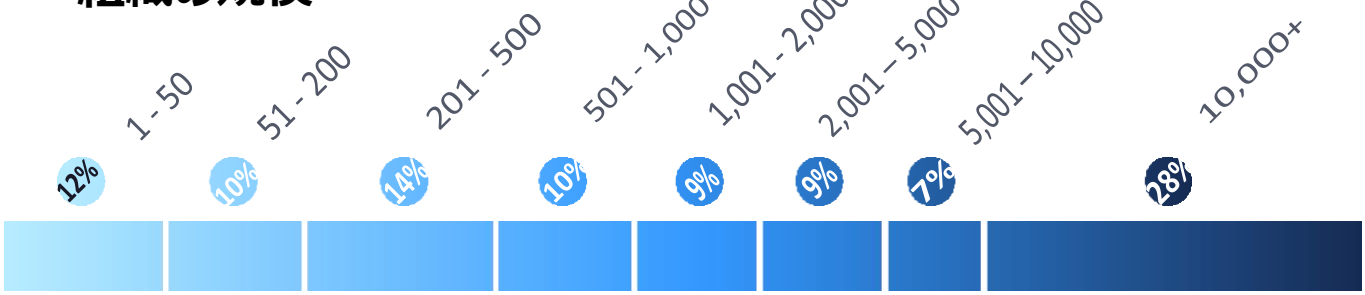
この調査は2021年5月から2021年6月まで実施され、さまざまな組織の規模、業界、場所、役割のITおよびセキュリティの専門家から1090件の回答が集められました。

組織の業界

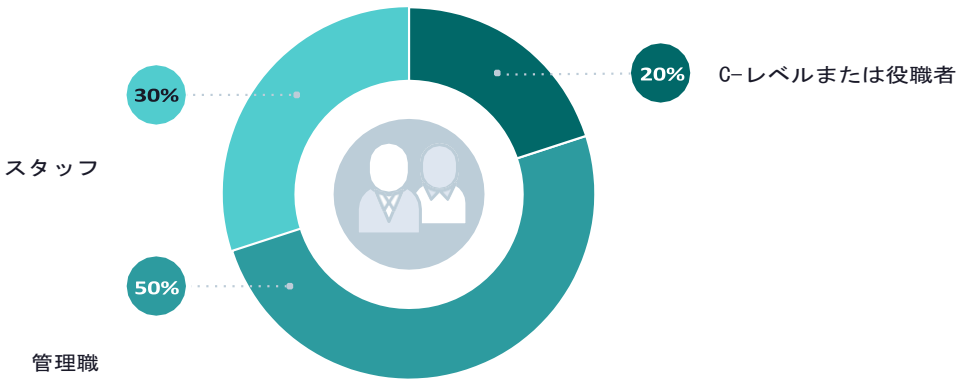


- 36% IT とテクノロジ
- 19% 金融サービス
- 16% 公共 (政府, 教育等)
- 9% ビジネスおよび専門サービス
- 6% その他
- 6% 健康, 医薬品, およびバイオテクノロジ
- 5% 通信
- 4% 製造業
- 3% 小売
- 2% 資源, 石油/ガス, 公共
- 2% 旅行, 交通機関
- 1% 建設, 不動産

組織の規模

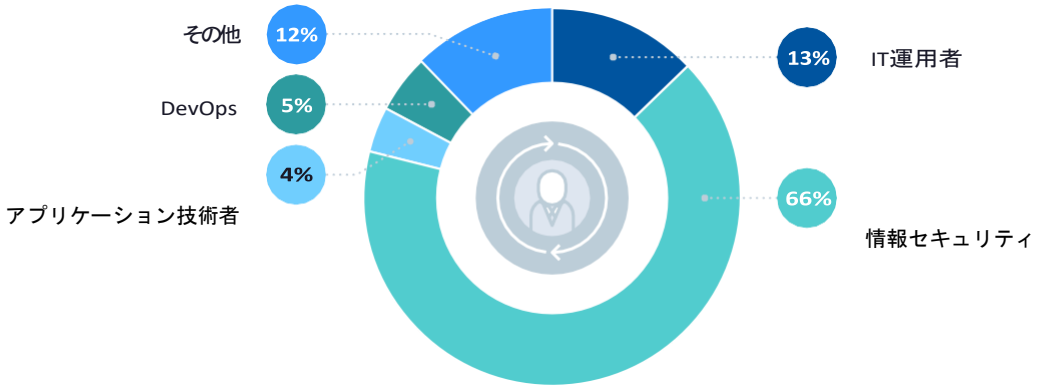


ジョブレベル

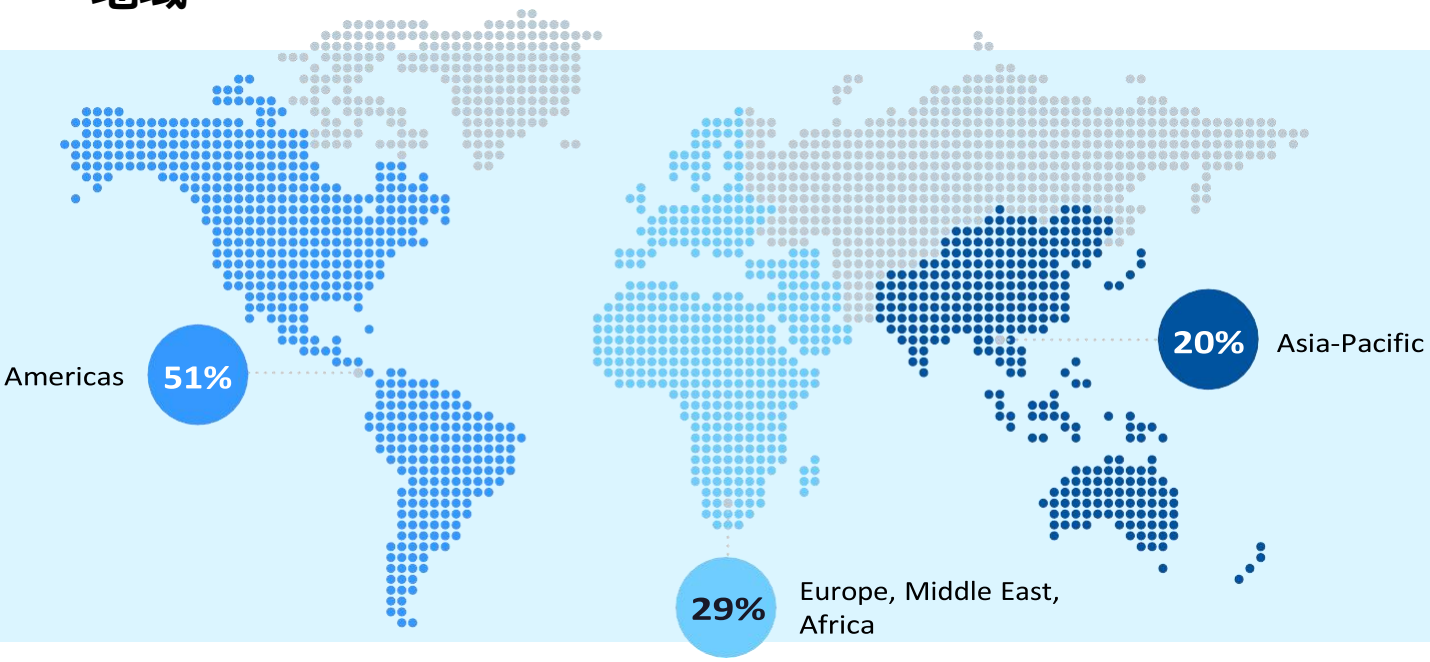


組織のパブリッククラウド支出

所属部門



地域



主な貢献国は次のとおりです。アメリカ合衆国、インド、イギリスおよび北アイルランド、カナダ、オーストラリア、シンガポール、ドイツ、スイス、フランス

スポンサーに関して

VMwareは、エンタープライズソフトウェアの主要なイノベーターです。私たちは世界のデジタルインフラストラクチャを強化しています。クラウド、アプリのモダナイゼーション、ネットワーキング、セキュリティ、デジタルワークスペースのプラットフォームは、柔軟で一貫性のあるデジタル基盤を形成します。この基盤により、企業はどこにいてもアプリケーションを構築、実行、管理、接続、保護できるようになり、テクノロジ主導の変革を中断することなく実現できます。VMwareは、2018年10月にCloudHealth Technologies,Inc.を買収しました。

CloudHealth by vmware®

スポンサーは、研究プロジェクトの調査結果をサポートするCSA法人会員ですが、CSA研究のコンテンツ開発または編集権に追加の影響を与えることはありません。