cloud security alliance®

valence

Survey Report

SaaS セキュリティの現状レポート

2025 年～2026 年の動向と洞察

The permanent and official location for the [Insert WG Name] Working Group is https://cloudsecurityalliance.org/research/working-groups/working-group-name

謝辞

Lead Authors

Hillary Baron

Contributors

Marina Bregkou
Josh Buker
Ryan Gifford
Alex Kaluza
John Yeoh

Graphic Design

Claire Lehnert
Stephen Lumpe

スポンサーについて

Valence は SaaS のリスクを発見し、修正します。Valence プラットフォームは、比類のない SaaS ディスカバリ、SSPM、および ITDR 機能を通じてシャドー IT、設定ミス、およびアイデンティティ活動を監視することにより、SaaS アプリケーションを発見、保護、防御します。最近話題となった情報漏えいは、分散型 SaaS の導入がいかに重大なセキュリティ課題を引き起こしているかを浮き彫りにしています。Valence を使用することで、セキュリティチームは SaaS の無秩序な拡大を制御し、データを保護し、人間および人間以外のアイデンティティからの疑わしい活動を検出することができます。Valence は可視化を超え、セキュリティチームがワンクリックでのリスク是正、自動化されたワークフロー、およびビジネスユーザーとの協業を通じてリスクを是正できるようにします。大手企業から信頼されている Valence は、今日の最も重要な SaaS セキュリティリスクを軽減しながら、SaaS のセキュアな導入を保証します。
https://www.valencesecurity.com

日本語版提供に際しての告知及び注意事項

本書「SaaS セキュリティの現状レポート 2025 年～2026 年の動向と洞察」は、Cloud Security Alliance (CSA)が公開している「The State of SaaS Security Trends and Insights for 2025-2026」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
2025年05月19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

「SaaS セキュリティの現状レポート 2025 年～2026 年の動向と洞察」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）

高橋　久緒
松浦　一郎, CISSP, CISM, CDPSE
満田　淳
諸角　昌宏
米山　努

目次

エグゼクティブサマリー

SaaS（Software-as-a-Service）アプリケーションはビジネス運営の基盤となっており、企業はより大きな投資と注意を払って対応しています。しかし、2025 CSA SaaS Security Survey では、優先順位が高まる一方で、可視性、アイデンティティ、及び、ガバナンスにおける中核的な課題は依然として残っており、SaaS セキュリティに対するより統合された目的別のアプローチの必要性が浮き彫りになっています。

主な調査結果

1.SaaS セキュリティに対する優先度の高まり
現在、SaaS セキュリティは 86% の組織にとって最優先事項であり、76% が予算を増やし、79% が自社のプログラムに自信を示しています。組織は、脅威の検出（50%）やポスチャ管理（47%）などの主要分野に注力しています。

2.機密データのリスク
データの過剰な共有と不十分なアクセス制御は、組織をリスクに曝し続けています。63%が外部との過剰な共有を報告し、56%が機密データが許可されていないアプリにアップロードされていると回答しています。

3.分散化した SaaS の導入と管理によるセキュリティギャップ
従業員の 55%がセキュリティ部門の関与なしに SaaS を採用し、57%が断片的な管理を報告していることから、多くの組織がチームやツール間で一貫した監視とポリシー施行の維持に苦慮しています。

4.自動化と一貫性に欠ける人的アイデンティティ管理
IAM は依然として課題であり、58%は権限の適用に苦慮しており、54%はライフサイクル管理の自動化が不十分です。これらのギャップは、情報漏えいに直結し、組織を脆弱な状態にしています。

5.SaaS 間統合と人間以外のアイデンティティは盲点
SaaS 間の統合と生成 AI ツールは、アタックサーフェスを拡大しています。組織の半数近く（46%）が人間以外のアイデンティティ（NHI）の監視に苦慮しており、56%が過剰な特権による API アクセスに関する懸念を報告しています。

6.現在のツールと戦略では全体的なセキュリティには不十分
自信があると言っているにもかかわらず、多くの企業はベンダー独自のツール（69%）、CASB のような汎用ソリューション（43%）、さらには手動監査（46%）に依存しています。こうした断片的な戦略では、SaaS 環境全体に重大なギャップが残ります。

重要なポイント

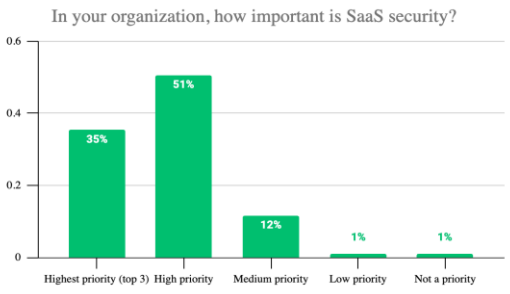
現在の SaaS セキュリティ戦略のほとんどは、未だリアクティブで断片化されたものであり、組織の機密データがリスクにさらされています。真にリスクを低減するためには、企業は、ディスカバリ、ポスチャ管理、脅威検出、アイデンティティセキュリティ、および修復にまたがる統合された機能への投資を一致させる必要があります。

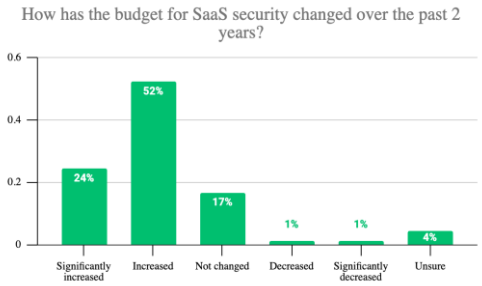
主な調査結果

SaaS は現代のビジネスオペレーションの中核となっていますが、そのセキュリティの確保は依然として難しい課題です。企業は、これまで以上に多くのクラウドベースのアプリケーションを採用する一方で、可視性のギャップやシャドーIT から、過剰な特権アクセスや未チェックのサードパーティ統合に至るまで、増大するセキュリティ上の課題に直面しています。脅威が進化し、SaaS 環境の相互接続が進むにつれて、セキュリティ戦略は受動的な監視から積極的なリスク削減へと移行する必要があります。問題は、SaaS のセキュリティが優先事項であるかどうかではなく、組織が実際に対応しているかどうかです。

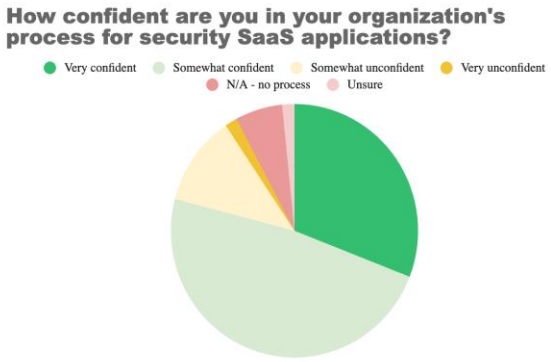
主な調査結果 1: SaaS のセキュリティは、企業が投資を拡大するにつれて優先度が高まっています

SaaS セキュリティの優先度はこれまで以上に高まっており、**86% の組織が優先度が高いまたは最も高いと回答しています**。これは CSA の 2024 年の調査で優先度が中程度から高いという回答が 80% から増加したことを示しており、より強固な保護の必要性に対する認識が高まっていることを反映しています。この優先順位付けに従って投資も進んでおり、**企業の 76%が今年、SaaS** セキュリティ予算を増額しています。2024 年に予算増額を報告した 39%のほぼ倍増です。





SaaS 環境が拡大し続ける中、企業はセキュリティにより多くの予算を割り当てるだけでなく、主要なリスク領域に焦点を絞るようになっています。**組織の半数（50%）が SaaS 脅威の検出を優先し**、さらに **47%が SaaS Security Posture Management（SSPM）ソリューションを優先し、31%が SaaS アプリケーションの検出を優先しています**。これは、セキュリティチームが SaaS アプリケーションの可視性と管理を強化する方法を積極的に模索していることを示しています。ディスカバリ、ポスチャ、及び脅威の検出と対応はすべて、包括的な SaaS セキュリティ戦略の中核をなすものです。SaaS 環境が複雑化するにつれて、これらの機能を連携させる戦略が、セキュリティとリスクを包括的に管理する上でより有利な立場になります。



同時に、セキュリティプログラムに対する自信も

依然として高く、**79%が自社の SaaS セキュリティプロセスに自信を示しており**、多くの組織が SaaS 関連のリスク管理において進展を感じていることがわかります。しかし、この自信は、意図した戦略や日々の運用の実態を十分に反映していない可能性があります。このことは、多くの組織が、大規模な SaaS セキュリティを効果的に管理する能力を過大評価している可能性を示唆しています。

こうした進歩にもかかわらず、**SaaS** のセキュリティ確保は依然として**複雑な課題**であり、特に組織が SaaS の展開に伴いセキュリティ戦略を追随させる際に顕著です。**SaaS セキュリティの専任担当者が不足している企業は 39%に上り**、多くのチームが専任のリソースや専門的なリソースを持たずに SaaS 環境の管理に取り組んでいることがうかがえます。SaaS セキュリティへの投資が拡大するにつれ、企業は、テクノロジーと専門知識の両方を含む総合的な戦略に確実に投資し、SaaS エコシステム全体で脅威を検出できる能力を強化し、ポリシーを実施し、またリスクを削減する必要があります。

今年の調査結果は、SaaS セキュリティの重要性を認識するだけでなく、脅威の検出とセキュリティポスチャの管理を優先して積極的に取り組むことで、SaaS セキュリティの優先順位付けと投資を強化する方向へと明らかにシフトしていることを示しています。SaaS の導入が加速する中、この勢いを維持することは、複雑化する SaaS の状況に合わせてセキュリティ戦略を確実に進化させるために不可欠です。

主な調査結果 2：SaaS 上の機密データは、不十分な可視性と脆弱なアクセス制御によってリスクにさらされています

このような SaaS セキュリティ投資の背後にある緊急性は、企業が直面しているデータ露出リスクを見れば明らかです。**企業の 63%は、機微データや機密データの外部への過剰な共有を最大のリスクとして挙げており**、**56%は、従業員が機微データを未認可な SaaS アプリケーションにアップロードしていると報告しています**。これらの調査結果は、組織が SaaS セキュリティにより多くのリソースを投入している一方で、多くの組織が環境全体の機微データを保護するために必要な基本的な保護の確立に苦慮していることを示唆しています。

このようなリスクの主な要因は、効果的でない特権とアクセス管理の実践です。**組織の 41%が、最小特権アクセスポリシーが効果的に実施されていないと報告しています。**つまり、ユーザーやシステムが過剰な権限を保持することが多く、データ漏えいや権限の乱用、内部脅威のリスクが高まっているのです。この課題は、人間のアイデンティティに限ったことではありません。生成 AI（GenAI）の統合は、新たな複雑性のレイヤーを導入しており、多くの場合、タスクを実行するために、複数のアプリケーシ

ョンにわたる機密データへの広範なアクセスを必要とします。**組織の 56%は、サードパーティベンダーや AI を搭載した SaaS ツールが、データへの過剰な API アクセスを獲得することを懸念しています。**

従来のツールとは異なり、生成 AI やサードパーティの統合は自律的に動作することが多く、データの移動や分析、アプリケーション間の接続、大規模な出力の生成などを行います。これらの機能は、誤ったパーミッションの設定や見落とされた統合の影響範囲を大幅に拡大する可能性があります。適切な監視がなければ、これらのツールはデータをリスクにさらしかねません。AI ツールやシステムが SaaS のワークフローに組み込まれるようになると、新しいタイプのユーザーだけでなく、セキュリティチームが理解し管理しなければならないまったく新しい挙動パターンが生まれています。しかし、潜在的な攻撃対象が拡大しているにも関わらず、同じような監視やライフサイクル管理が適用されていません。

DeepSeek のようなオープンソースの生成 AI ツールの出現は、こうした懸念をさらに増幅させています。これらのツールは強力な機能を提供する一方で、IT やセキュリティの監督なしに採用されることが多く、十分なプライバシーとセキュリティ管理が行われていません。特に DeepSeek は、安全対策への投資が最小限に抑えられていることや、中国企業が政府当局と情報を共有することが法的に義務付けられていることから、警戒が高まっています。このようなリスクがあるにもかかわらず、DeepSeek のようなツールはあらゆるブラウザから自由にアクセスできるため、従業員による無許可の使用が可能です。このため、適切な監視や実施なしに機密データが漏洩する可能性が高まり、企業が SaaS 環境を管理し続けることがさらに難しくなります。

SaaS のデータフローが一元的に可視化されておらず、SaaS 間の統合が監視されていないことがこうした課題をさらに深刻にしており、**企業の 42% が SaaS アプリケーション全体の機微データの追跡と監視に苦慮しています**。明確な監視がなければ、セキュリティチームは、コンプライアンスポリシーの実施、未認可なデータ移動の検出、リアルタイムでのリスクへの対応といった課題に直面します。このような可視性のギャップは、脆弱なアクセス制御やサードパーティとの統合の急速な拡大と相まって、多くの組織が自社の SaaS の状況を根本的に理解していないことを示唆しています。

SaaS セキュリティの優先順位は高まっており、多くの組織がセキュリティポスチャを強化するために予算を増やしていますが、こうしたリスクに対処するには、単なる追加投資以上のものが必要です。特に GenAIVisibility の時代においては、より統合的で体系的なアプローチが求められます。SaaS 環境の可視化、最小特権アクセスの実施、アプリケーション間のデータ移動の一貫した監視は不可欠な第一歩です

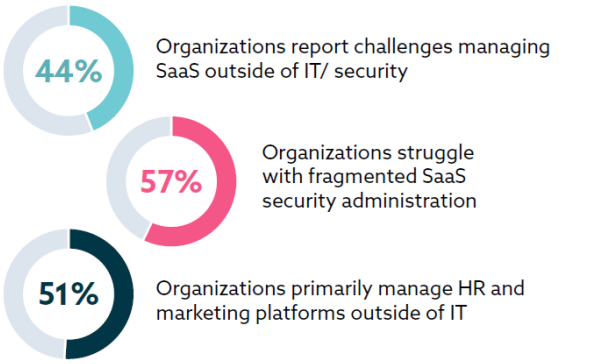
が、セキュリティ戦略は断片的なままであり、SaaS エコシステム全体へ包括的に適用されるのではなく、アプリケーションごとに適用されることが多くなっています。SaaS セキュリティの強固な基盤と、より統一された戦略がなければ、企業は機微データの保護、サードパーティのリスク管理、セキュリティ投資を単体の修正としてではなく、意味のある永続的な改善へ繋げることに苦労し続けるでしょう。

主な調査結果 3：分散型 SaaS の導入と管理の台頭（とリスク）

SaaS の導入が加速する中、従業員がセキュリティや IT 部門の関与なしにアプリケーションを導入するケースが増えており、こうしたツールの効果的な追跡、保護、および統治が難しくなっています。**組織の 55 パーセントが、従業員がセキュリティ部門の関与なしに SaaS アプリケーションにサインアップしていると報告しており**、機微データが監視されていない環境に流れ込むことで、新たなリスクが発生しています。このような分散型の導入は、ビジネスチームに柔軟性を提供する一方で、セキュリティの盲点を生み出し、どのようなアプリケーションが使用され、どのように設定され、機微データがどこに保存されているのか、組織が把握できないままになっています。

SaaS の導入だけでなく、SaaS の管理自体も IT 部門やセキュリティチームの外部に移行することが多く、その結果、セキュリティ監視に一貫性がなくなっています。**組織の 44% が IT/セキュリティ部門以外での SaaS 管理に課題を感じており、57% が SaaS セキュリティ管理の分断に悩んでいます**。この課題は、**機微性の高いデータを含むことが多い人事およびマーケティングプラットフォームで**特に問題となります。これらのアプリケーションは、51%の組織で主に IT 部門以外によって管理されています。ガバナンスへの一元的なアプローチがないと、セキュリティポリシーが矛盾して適用されることが多く、設定ミスのリスクやセキュリティインシデントへの対応の遅れが生じます。

SaaS management shifting causes inconsistencies in security oversight



Difficulties addressing SaaS risks

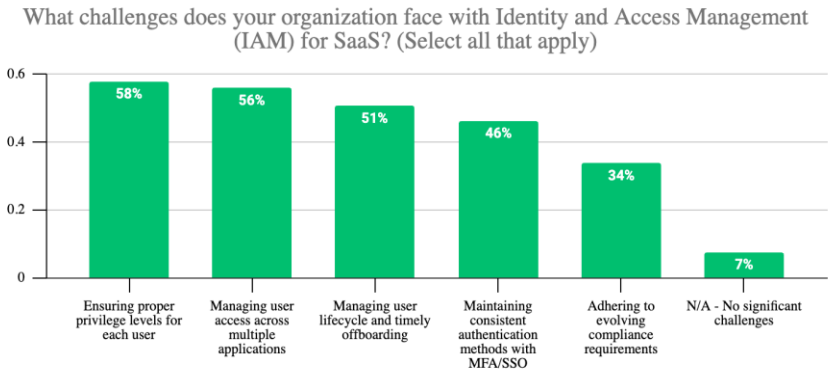
さらに複雑な課題は、セキュリティ、IT、及びビジネスチーム間のコラボレーションの障壁が、SaaS リスクへの対処をさらに困難にしていることです。**組織の 41% が、SaaS リスクを是正するための最大の障壁としてコラボレーションの問題を挙げており**、**35% が SaaS セキュリティに関するビジネス部門との具体的な協力の難しさを報告しています**。セキュリティの責任が複数のチームに分散している一方で、明確なオーナーシップがないため、責任の所在があいまいになっています。その結果、ポリシーの実施にギャップが生じ、セキュリティ管理に一貫性がなくなり、誰がリスク軽減の責任を負うのかが不明確になります。

組織の SaaS セキュリティには、明確なガバナンスと一元的な監視を重視した、より体系的で積極的なアプローチが必要です。SaaS の導入には常に複数のチームが関与することになりますが、セキュリティの責任は最初から明確に定義しておく必要があります。SaaS セキュリティの一貫した統一戦略がなければ、断片的な管理によって可視性のギャップ、ポリシーの不整合、セキュリティの盲点が生じ続けることになります。同様に重要なのは、ビジネス部門とセキュリティチームとの連携を強化することです。これらの利害関係者と信頼できるパートナーシップを確立することで、セキュアなオンボーディング、モニタリング、アクセス制御のプロセスの組織全体での遵守を確実にします。この転換がなければ、分散型モデルは管理されないリスクをもたらし続け、SaaS セキュリティは、まとまりのある協調的な戦略ではなく、一貫性のないポリシーのパッチワークになってしまいます。

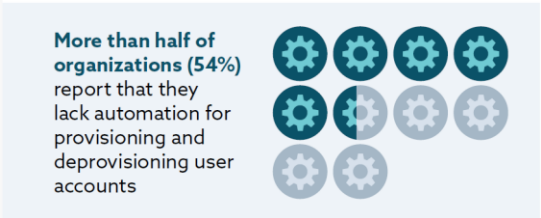
主な調査結果 4：SaaS における人的 ID 管理は、依然として持続的かつ拡大するセキュリティ上の課題

強固なアイデンティティとアクセス管理（IAM）は、SaaS 環境のセキュリティ確保に不可欠です。しかし、IAM の実装方法には一貫性がなく、SaaS アプリケーション全体で自動化が進んでいないため、IAM は根強い課題となっています。

この課題の最大の要因の 1 つは特権管理であり、**58%の組織が SaaS アプリケーション全体で適切な特権レベルの適用に苦慮しています**。一貫した特権付与が行われないと、ユーザーが必要以上の権限を保持する可能性があり、データ漏洩や内部脅威のリスクが高まります。この課題をさらに深刻にしているのは、**56%の企業が複数の SaaS アプリケーションにまたがるユーザーアクセスの管理に苦慮していることです**。これは、各 SaaS アプリケーションが独自のアクセスモデルと役割ベースの制御を持つ場合に、アイデンティティの可視性と制御を維持することがいかに困難であるかを浮き彫りにしています。このような矛盾はアイデンティティの乱立につながり、セキュリティチームが統一されたポリシーを実施し、潜在的な脅威に迅速に対応することを困難にしています。



アクセス管理は、アイデンティティ・ライフサイクル・プロセスの自動化不足によってさらに複雑化しています。**半数以上の組織（54%）は、ユーザアカウントのプロビジョニングとプロビジョニング解除の自動化ができていないと回答しています**。その結果、孤立したアカウントや権限の蓄積、不正アクセスのリスクが高まっています。これは、**タイムリーなオフボーディングを含むアイデンティティ・ライフサイクル・プロセスの管**



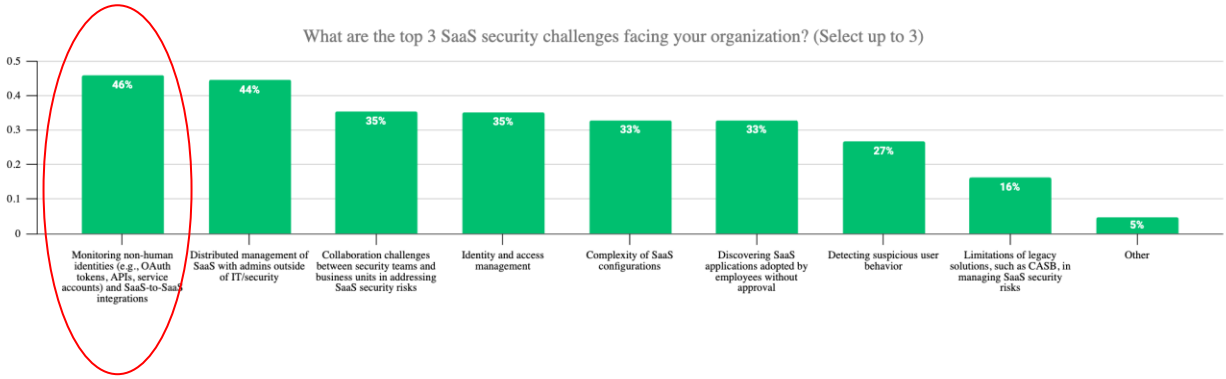
理に苦慮している組織が 51%に上る一因と考えられます。自動化されたライフサイクル管理がなければ、セキュリティチームは、非効率的でミスが発生しやすく、成長する SaaS エコシステム全体に対応するのが困難な手動プロセスに頼らざるを得ません。

こうした IAM の失敗は、単なる仮想的なリスクではありません。**SaaS 侵害の 46% は、脆弱な MFA 保護またはエクスプロイトされた MFA 保護 に関連しており、41% は過剰な特権アカウントに起因しています**。組織が多要素認証（MFA）の実施、最小特権の適用、 アイデンティティガバナンスの実施に苦慮している場合、攻撃者はセキュアでないアクセス、設定ミス、過剰な権限、またはセキュアでないアカウントを利用して、SaaS アプリケーション間を横移動することができます。これはデータ侵害の可能性を高めるだけでなく、インシデントレスポンスも複雑にします。断片的なアイデンティティ管理では、重大な被害が発生する前に不正アクセスを検出して封じ込めることが難しくなるからです。MFA が重要な防御手段であることに変わりはありませんが、特に、アクセスのプロビジョニングや特権管理などの基本的なプロセスに一貫性がなかったり、不完全であったりする場合は、アイデンティティ関連のリスクに完全に対処することはできないことを覚えておくことが重要です。

SaaS 環境における IAM の複雑化は、SaaS セキュリティを断片化する主な要因です。従来の IAM モデルとは異なり、SaaS のアイデンティティセキュリティは、それぞれ固有の認証と役割構造を持つ何百ものアプリケーションを考慮する必要があります。一元化されたアプローチがなければ、組織は規模に応じたアクセス制御の実施に苦労し続け、SaaS セキュリティの取り組みを弱体化させるセキュリティギャップを残すことになります。リスクを低減するために、組織は、最小特権の原則を徹底し、ユーザーライフサイクル管理を合理化し、すべての SaaS アプリケーションに一貫した監視機能を提供する SaaS セキュリティソリューションを採用する必要があります。これらの機能をより広範な SaaS 戦略に統合することができれば、アイデンティティ関連のリスクを管理する体制が整い、断片的なセキュリティ戦略による複合的な影響を回避できます。

主な調査結果 5：人間以外のアイデンティティと SaaS 間統合は拡大するセキュリティの盲点

IAM の課題は人間のアイデンティティだけではありません。人間以外の ID（NHI: non-human identities ）の監視と保護もますます難しくなっています。**企業の 46 パーセントが、 NHI のモニタリングを最大の課題として挙げています**。組織は、特権の行使、アイデンティティの乱立、ユーザーのライフサイクル管理に苦慮しています。これらと同じ課題が、API ベースの接続、OAuth トークン、サービスアカウントにも当てはまり、さらに複雑な方法をとることも多くなります。



SaaS 間統合の急成長の主な要因は、生成 AI とコパイロット化されたアプリケーションの台頭です。これらのツールはしばしば自律的に動作し、人間の介入なしにアクションを実行し、データを取得し、ワークフローを起動します。**組織の 56 パーセントが、サードパーティベンダーと生成 AI ツールは機密データへの API アクセスを過剰に許可されていると報告しており**、過剰な許可と可視性と監視の欠如の組み合わせがいかにリスクをもたらすかを強調しています。これらの統合は、一度設定されると放置されることが多く、不正アクセスやデータ流出のためにエクスプロイトされる可能性のある、監視されていない接続の蓄積につながります。

生成 AI とエージェント型 AI ツールは、セキュリティの状況をさらに複雑にしています。設計上、これらのシステムは、アプリケーション全体で大量のデータを取り込み、相互作用するように構築されているため、デフォルトで広範なアクセス権限が必要です。これらのツールが適切なガバナンスなしに導入された場合、意図した範囲を超えて機密情報にアクセスしたり、変更したりする可能性があります。伝統的なサービスアカウントとは異なり、生成 AI 主導のツールは、しばしば人間と機械のアクティビティ

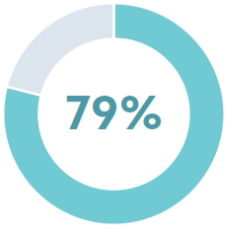
間の境界線を曖昧にし、SaaS のための従来の IAM アプローチを使用して追跡することを困難にしています。

NHI の普及が進んでいるにもかかわらず、人間のアカウントと同じような厳格なガバナンスが適用されることはほとんどありません。NHI のセキュリティとガバナンスは、組織の広範な SaaS セキュリティ戦略に統合されなければなりません。NHI 専用の可視化、ライフサイクル管理、ポリシーの適用がなければ、セキュリティチームは状況を把握できず、重要なアクセスポイントがチェックされないまま運用されることになります。NHI が SaaS アプリケーションの相互作用の中心的な役割を果たすようになるにつれ、その管理を見過ごすと、セキュリティ環境がさらに断片化され、一貫性のない保護が生み出されるため、SaaS セキュリティポスチャの強化が難しくなります。

主な調査結果 6：現在の SaaS セキュリティ戦略への過信が覆い隠すギャップ

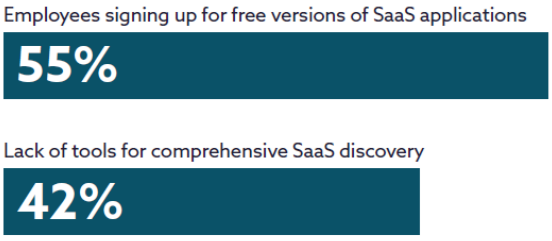
SaaS セキュリティの優先度が高まっていることは明らかですが、多くの組織では、SaaS セキュリティを効果的に管理するために必要な統合戦略や専用ツールがまだ不足しています。**SaaS セキュリティプログラムに**自信を持っていると**回答した企業は** 79%と依然として高い水準に**ありますが、**その自信が重大な能力ギャップを覆い隠している可能性があります。セキュリティ対策は、一貫性のないツール、サイロ化されたプロセス、限られた可視性の寄せ集めになっていることが多く、SaaS 環境を総合的に保護する能力が損なわれています。

Confidence in SaaS security programs

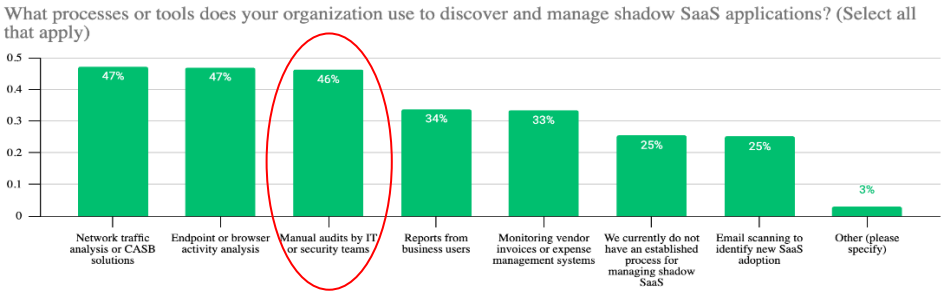


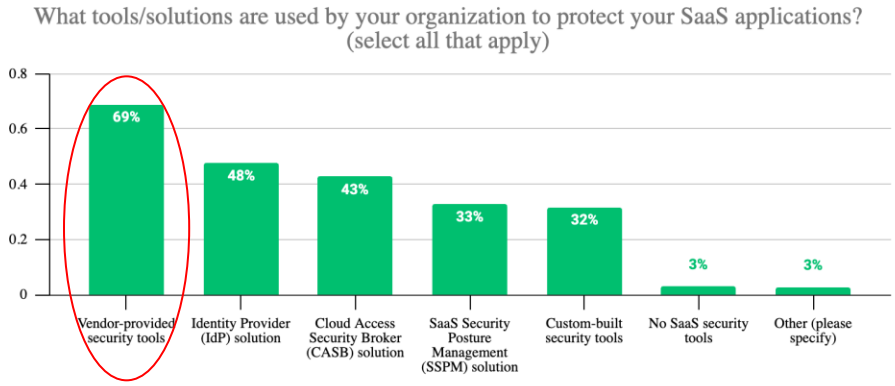
ディスカバリは、多くの組織の SaaS セキュリティ戦略における基本的なギャップの 1 つとして残っています。SaaS が乱立しているにもかかわらず、**組織の 42% が包括的な SaaS ディスカバリ機能がないと回答しており**、どのアプリケーションが使用されているか、機密データがどこに存在するか、ユーザーがこれらのアプリケーションとどのようにやり取りしているかなどの可視性が制約されています。ディスカバリは、SaaS のセキュリティを確保するために不可欠な最初のステップであるだけでなく、ポスチャ管理、脅威検出、リスク緩和をサポートする継続的な機能です。ディスカバリがなければ、組織は盲目的に運用することになり、設定ミスを特定したり、一貫したポリシーを適用したり、未承認のツールがセキュリティ上の障害になる前に検出したりすることができません。**組織の 55% が、従業員が未認可の SaaS ツールや無料の SaaS ツールにサインアップしており**、管理されていないリスクが発生し、セキュリティチームが効果的に監視またはコントロールできる範囲を超えたアタックサーフェスが拡大して**いると報告している**ことは、驚くべきことではありません。

What are the biggest challenges your organization faces in identifying all SaaS applications in use?

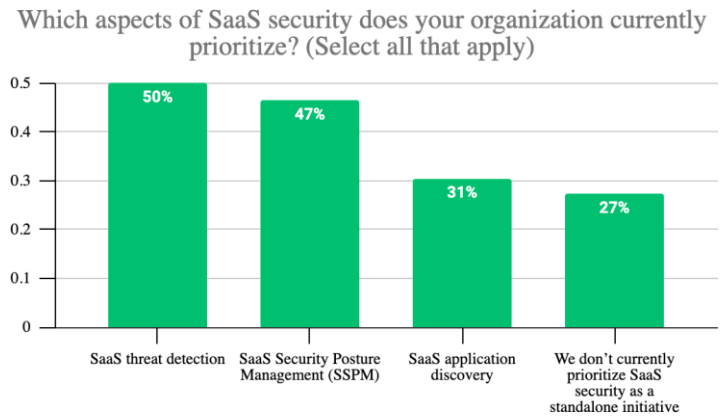


SaaS の導入が急速に進み、複雑化しているにもかかわらず、**組織の 46% が依然として SaaS リスクの管理を手作業による監査に頼って**おり *（訳注：本データを説明する図が原文には示されていませんので追加しました）*、これは動的でアプリ主導の環境には適さない、対処的かつリソースを多く消費する方法です。**さらに、組織の 69%は、**個々の SaaS アプリケーション内で**ベンダーが提供するネイティブのセキュリティ機能に依存しています**。このようなアプローチでは、広範な SaaS 環境全体でコントロールが孤立したり、保護に一貫性がなくなったりすることがよくあります。最近の Snowflake の顧客情報漏えいは、ベンダーが提供するネイティブな管理機能だけに依存することがなぜ危険なのかを思い起こさせるものでした。組織は、プロバイダがセキュリティのあらゆる側面を処理するであろうと仮定すると、アイデンティティガバナンス、API モニタリング、または脅威検出などの重要な責任を見落とす可能性があります。このケースに見られるように、信頼できるプロバイダであっても、内部の設定ミスや監視が不十分であれば、組織を侵害から完全に保護することはできません。これは、責任共有モデルの重要性と、組織が独立した可視性とコントロールを維持する必要性を補強します。





また、カバー範囲を拡大するために、**アイデンティティプロバイダ（IdP）（48%）や Cloud-Access Security Broker（CASB）（43%）など**、より一般的なクラウドセキュリティソリューションに目を向けている企業も少なくありません。これらのツールは、より広範なセキュリティアーキテクチャにおいて重要な役割を果たしますが、組織が現在直面している SaaS 固有の課題に対処するには適していない可能性があります。本レポートと「2024 CSA SaaS Security Survey」の両方で強調されているように、断片的なアプローチに依存し続け、アプローチの転換がなければ、SaaS 環境がより複雑化するにつれて、こうしたギャップは解消されず、むしろ拡大する可能性があることを示唆しています。



明るい兆候として、組織は自身の最も差し迫った課題に一致するソリューションを優先し始めています。**50% が SaaS 脅威の検出を、47% が SaaS Security Posture Management（SSPM）を、31% がアプリケーションの検出を優先しています**。これらの傾向は、従来のアプローチから、よりプロアクティブな考え方、つまり、SaaS エコシステム全体のセキュリティを確保するためには、可視化、コントロール、および対応機能のすべてが連携して機能する必要があることを認識する考え方へとシフトしていることを示しています。全体として見ると、SaaS のセキュリティ戦略が断片的で、リアクティブで、不完全なままであることが示されています。増大する投資と実際の能力とのギャップを埋めるには、企業は、アプリごとの場当たり的な管理から、検出、ポスチャ管理、脅威の検出、及びリスクの緩和といった中核的な課題に対処する、より統合的なアプローチへと移行する必要があります。SaaS セキュリティの全体的な最優先事項としての地位向上とともに、SaaS の脅威検出とポスチャ管理の優先順位が高まっていることは、多くの組織が現在の課題に対処し、より全体的かつ協調的な戦略を策定する準備が整っていることを示しています。

結論 SaaS セキュリティは現在進行形

SaaS セキュリティは組織の最優先事項となっており、予算配分が増加し、脅威の検出やポスチャ管理などの中核分野への注目が高まっています。各組織は、業務インフラストラクチャーにおける SaaS の重要性を認識し、そのセキュリティ対策に取り組んでいます。しかし、SaaS セキュリティプログラムに対する信頼は高いものの、多くの組織では成熟した拡張可能な SaaS セキュリティ戦略の構築に向けては、まだ初期段階にあることが示唆されました。

このような緊急性を駆り立てるリスクは現実のものです。機密データが SaaS 環境を通じて流れているにもかかわらず、多くの企業は最小特権アクセスの実施や、データの保存場所や共有方法の追跡に苦慮しています。過剰な共有、未認可のアップロード、サードパーティの過剰なアクセスは、データのライフサイクル全体における可視性とコントロールの欠如を意味します。ガバナンスを強化し一元的な監視を行わなければ、このようなギャップにより機密データは内部のミスや外部からの脅威に対して脆弱なままになってしまいます。

同時に、SaaS の導入と管理が分散化していることが、セキュリティへの取り組みを複雑にしています。従業員はセキュリティ部門の関与なしにアプリケーションを導入し、人事やマーケティングなどの重要なプラットフォームは IT 部門の関与なしに全般的に管理されることがよくあります。このため、SaaS アプリケーションの導入、設定、及びモニタリングの方法に一貫性がなく、特定のチームがプロセスを終始管理することができないため、セキュリティの責任に漏れが生じてしまいます。協力体制と責任の明確化は、リスクを是正するための最大の障壁の 1 つとして残っており、多くの組織は、プロアクティブなセキュリティポスチャではなく、リアクティブな対応を余儀なくされています。

これらの課題は、人間と人間以外のアイデンティティの両方にまたがるアイデンティティ関連の問題によって、さらに複雑になっています。人間の IAM は、一貫性のない特権管理とアイデンティティライフサイクルプロセスの自動化不足により、依然として根強い問題です。OAuth トークン、API 接続、ますます自律的になる生成 AI ツールなど、人間以外のアイデンティティは、さらに複雑なレイヤーを追加します。このような統合は、従来の IAM の範囲外で運用されることが多く、監視されない過剰な特権を持つ経路を生み出し、アタックサーフェスを拡大し、検知を回避します。

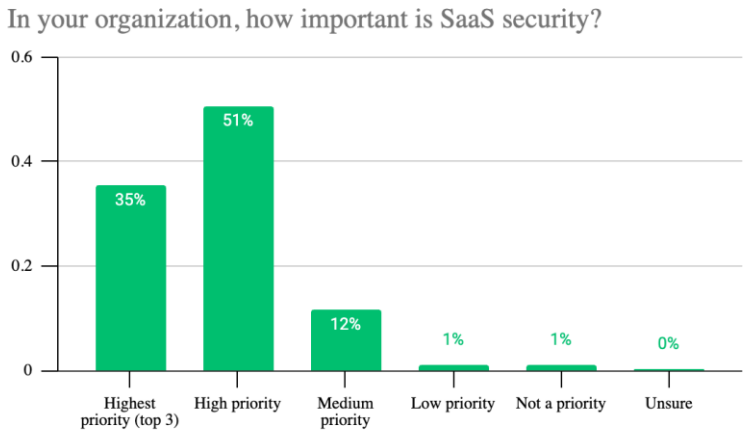
これらの調査結果を総合すると、SaaS セキュリティは依然として後回しにされていることがわかります。優先順位付けと投資において明確な進展が見られるにもかかわらず、ほとんどの企業は、手作業による監査、汎用的なクラウドセキュリティソリューション、ネイティブアプリレベルの管理など、SaaS の現実を想定して構築されていないツールや戦略に依存しています。ほとんどの組織は、不完全な適用範囲と一貫性のない実施で対応しているため、環境は無防備な状態に置かれ、自信は過信に陥っている可能性があります。

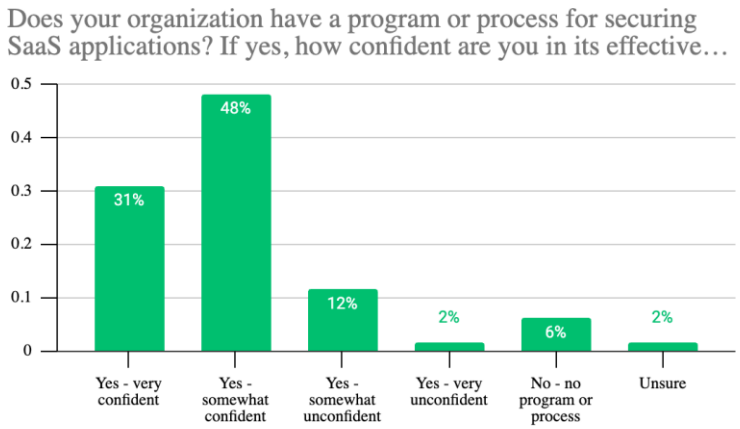
SaaS と AI のイノベーションのスピードに対応するためには、企業は今すぐ行動を起こす必要があります。そのためには、SaaS のセキュリティを、単なる個別のアプリケーションの集合ではなく、エコシステムとしてサポートするために、どのようなツール、戦略、およびプラクティスが最適かを理解し、認

識を深めることから始めなければなりません。ディスカバリの改善、自動化されたポスチャ管理、プロアクティブなリスク検出など、より統合的で将来を見据えたアプローチが必要です。SaaS の導入は加速する一方であり、このような基本的な課題に対処するための時間は急速に限られてきています。

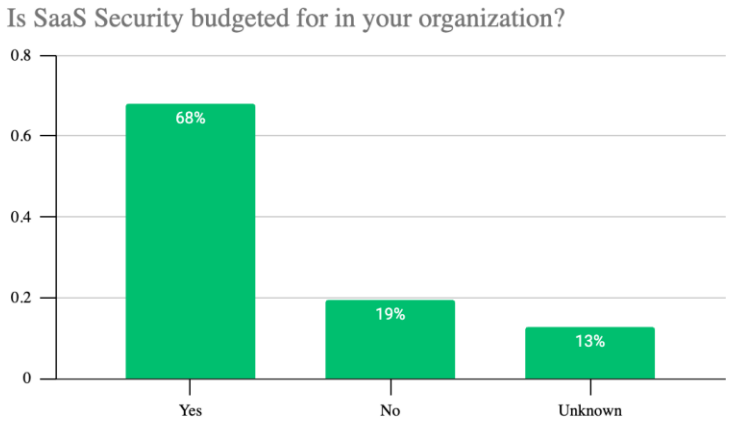
全サーベイレポート

概要

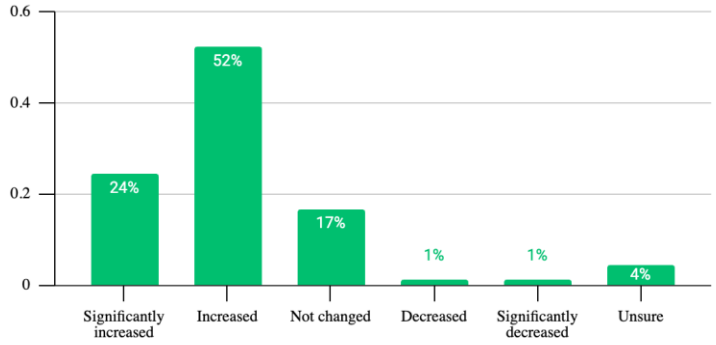




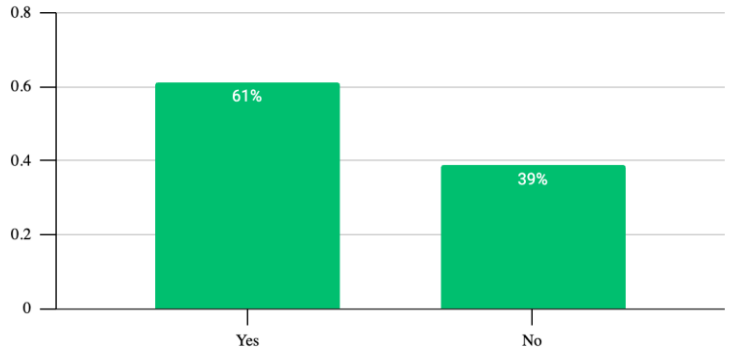
SaaS セキュリティプログラム



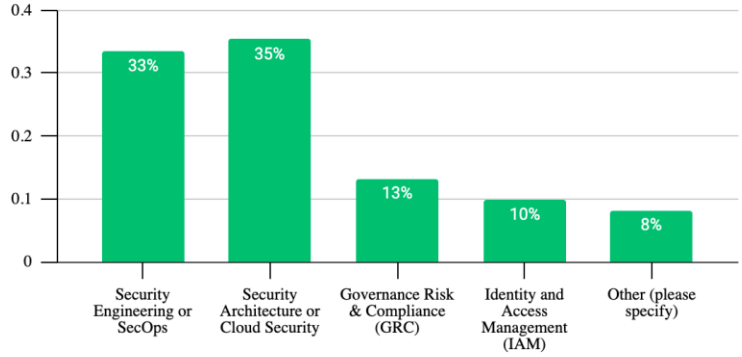
How has the budget for SaaS security changed over the past 2 years?

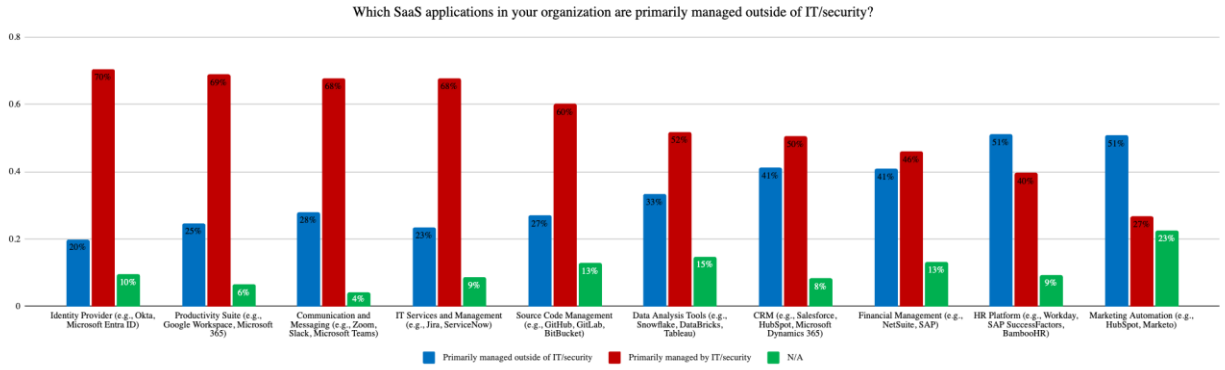


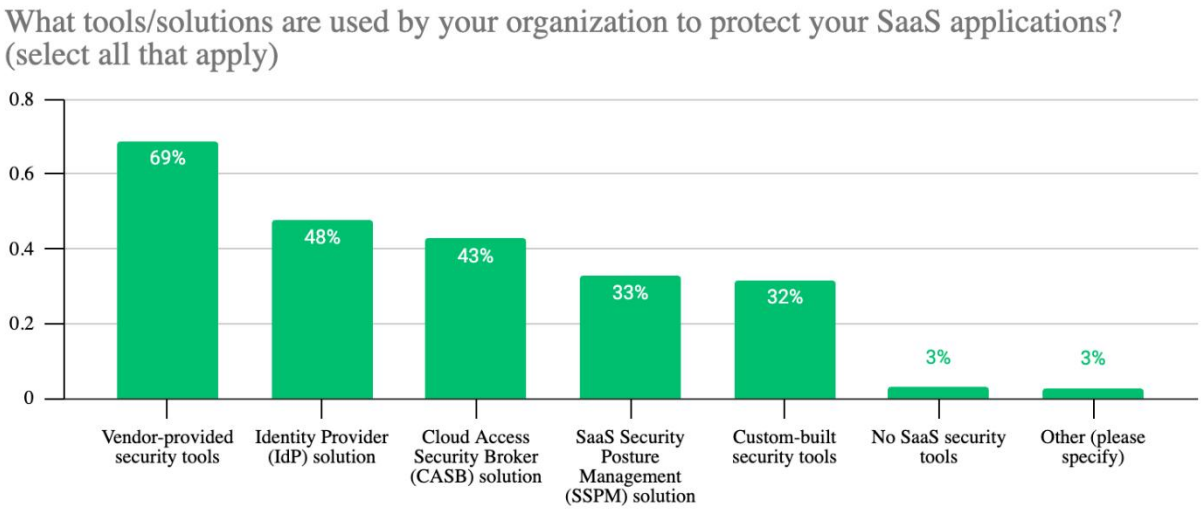
Does your organization have specific personnel focused on SaaS security?



Which team is primarily responsible for SaaS security in your organization?

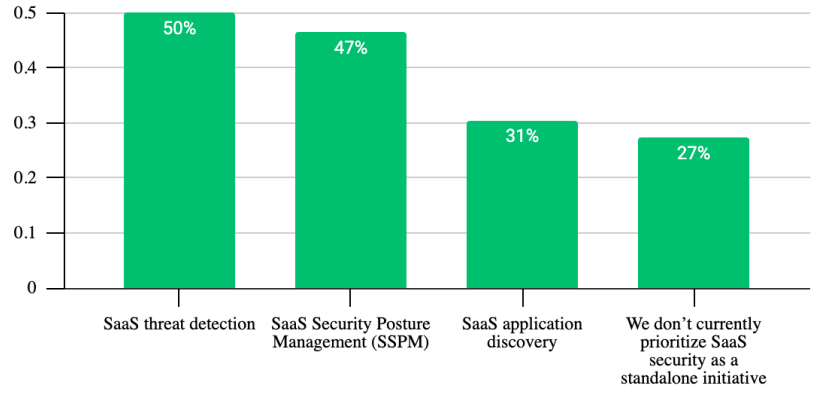




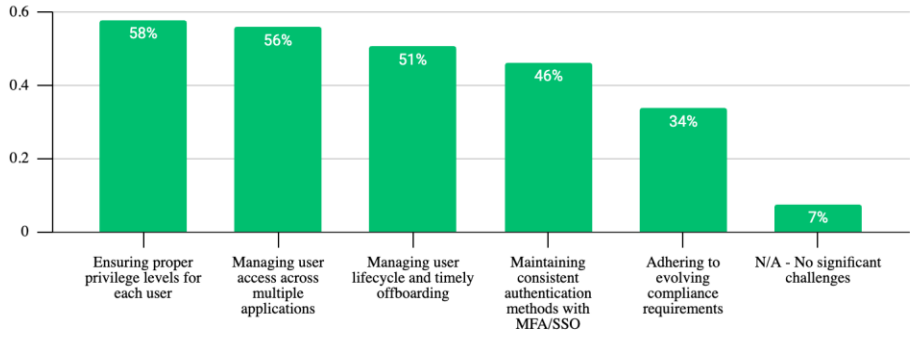


優先順位と課題

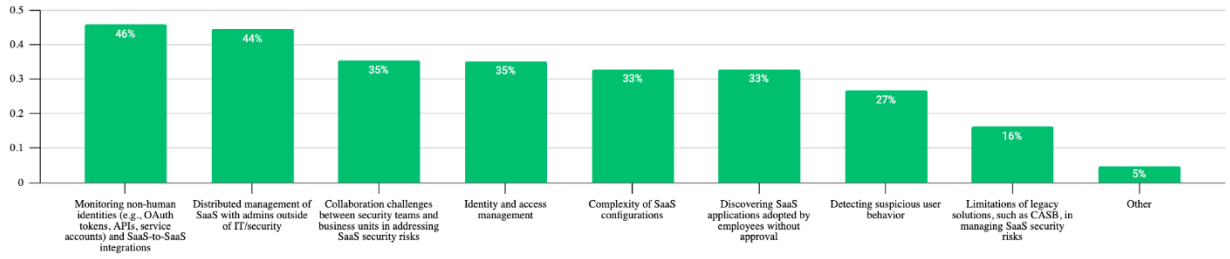
Which aspects of SaaS security does your organization currently prioritize? (Select all that apply)

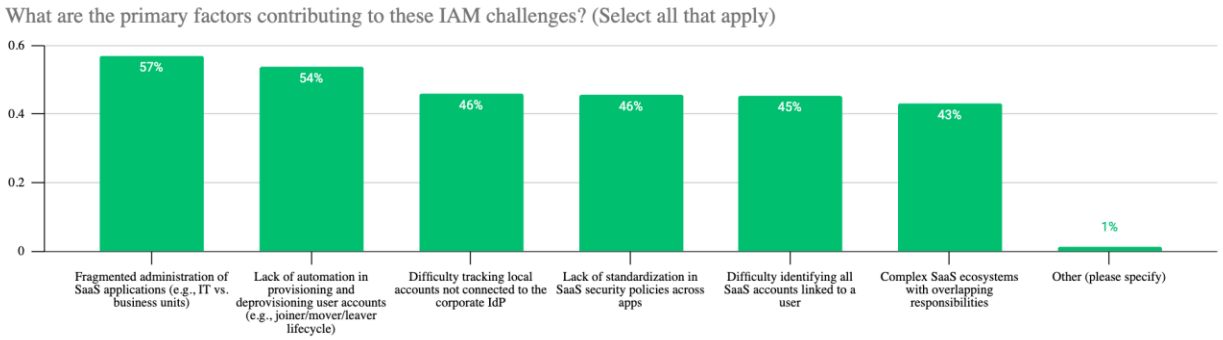


What challenges does your organization face with Identity and Access Management (IAM) for SaaS? (Select all that apply)

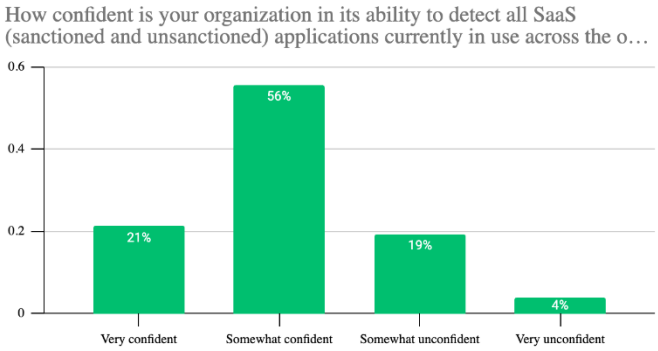


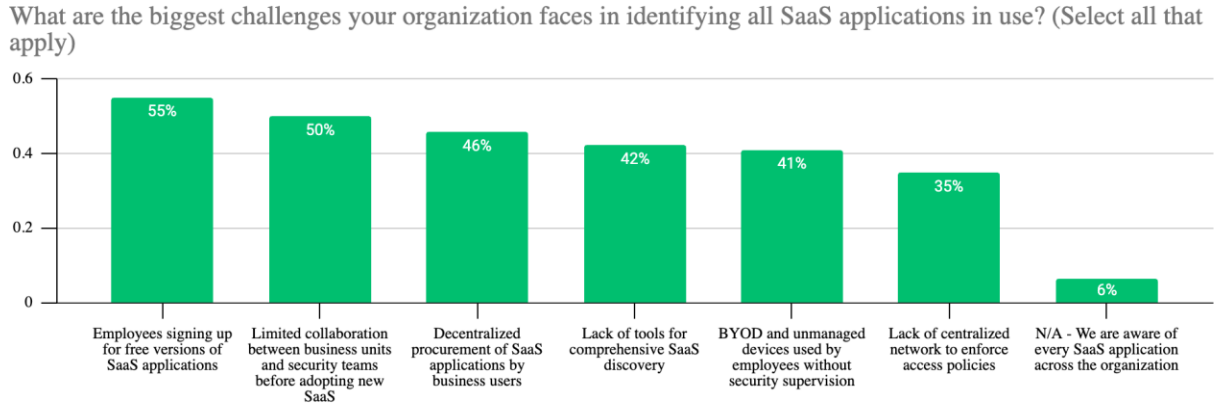
What are the top 3 SaaS security challenges facing your organization? (Select up to 3)



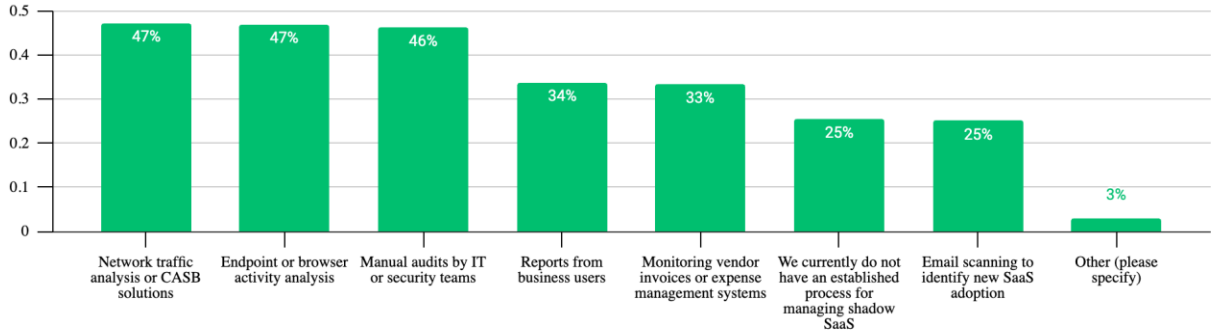


SaaS ディスカバリ



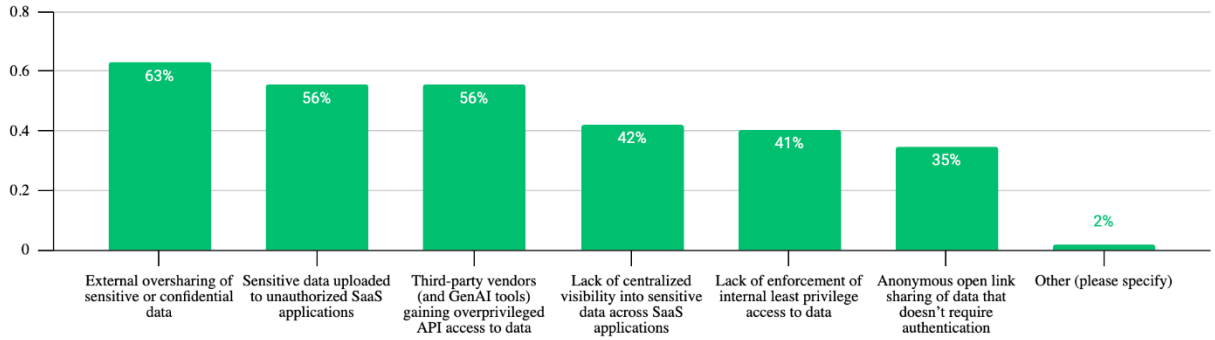


What processes or tools does your organization use to discover and manage shadow SaaS applications? (Select all that apply)

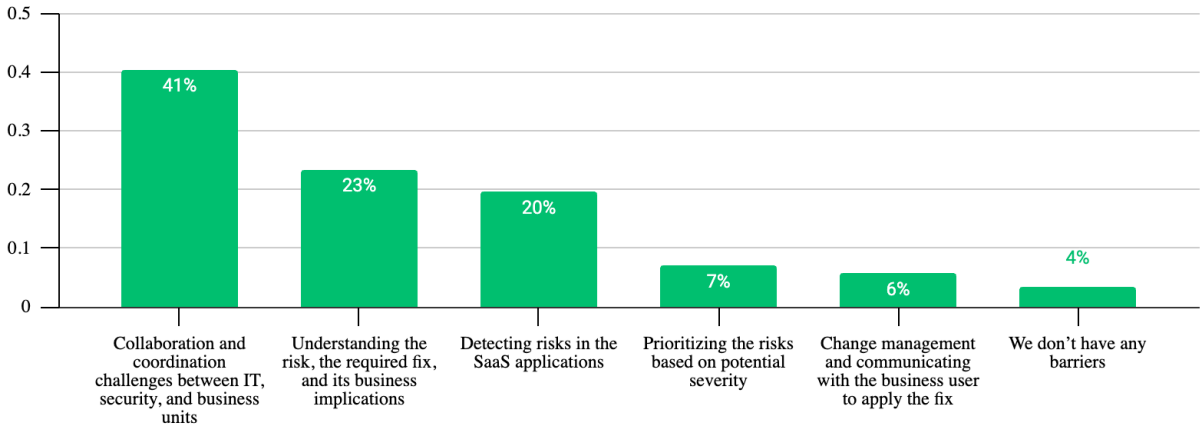


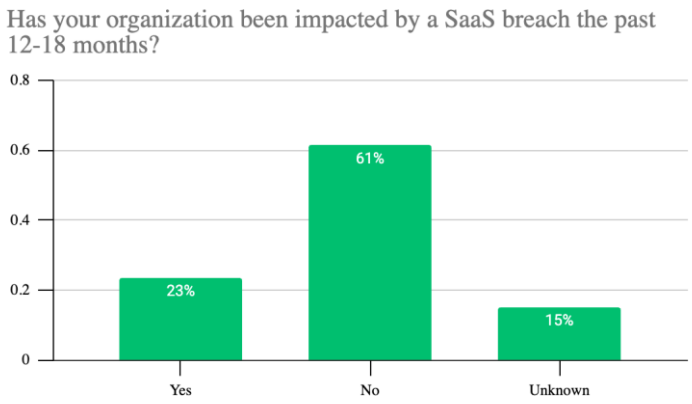
SaaS セキュリティインシデント

What are the most significant data exposure risks your organization faces in SaaS applications? (Select all that apply)



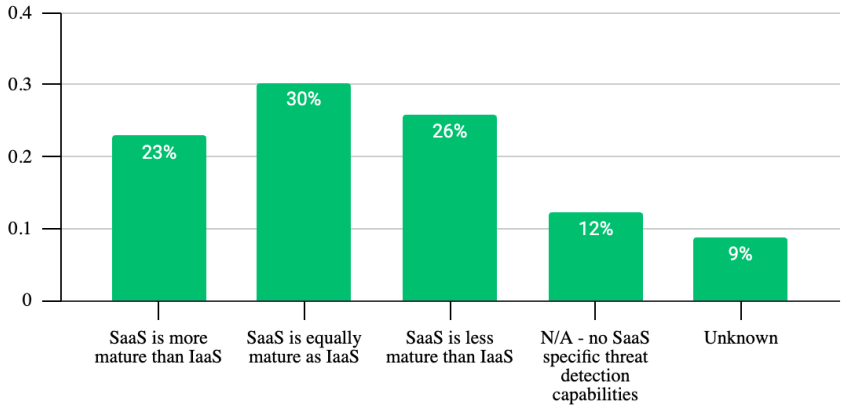
What is the largest barrier to remediating SaaS risks in your organization?



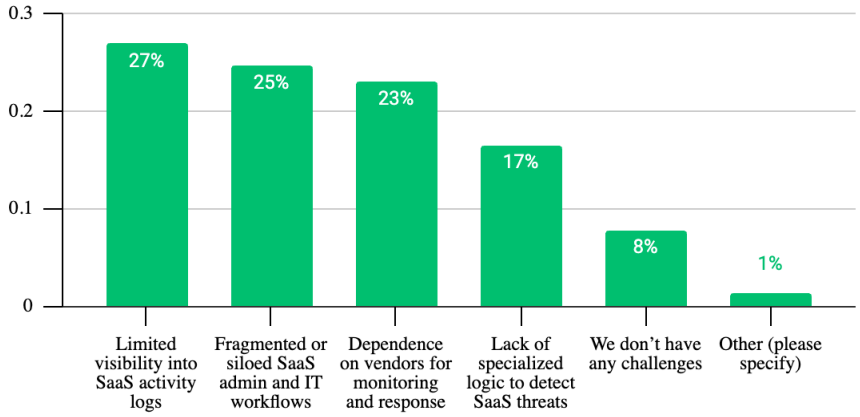


SaaS の検出と応答

How does your organization's SaaS threat detection and response capabilities compare to those for IaaS?



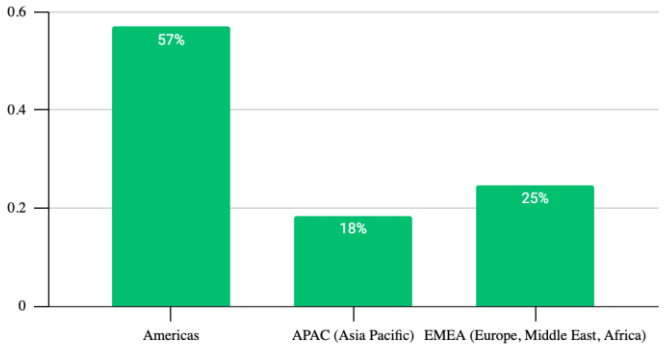
What is the biggest challenge your organization faces in detecting and responding to SaaS-specific threats?



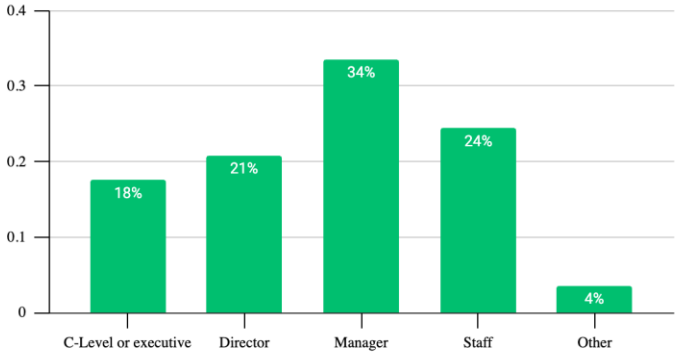
統計データ

この調査では、業種、規模、および地域が異なるさまざまな組織の IT およびセキュリティの専門家 420 人から洞察を得ました。人統計データの内訳は、調査結果を理解する上で重要な背景となり、さまざまな部門や業務規模の組織が直面するさまざまな経験や課題を浮き彫りにします。

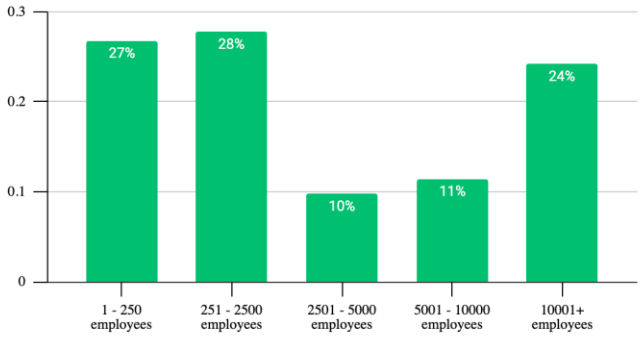
Select which region you are located in.



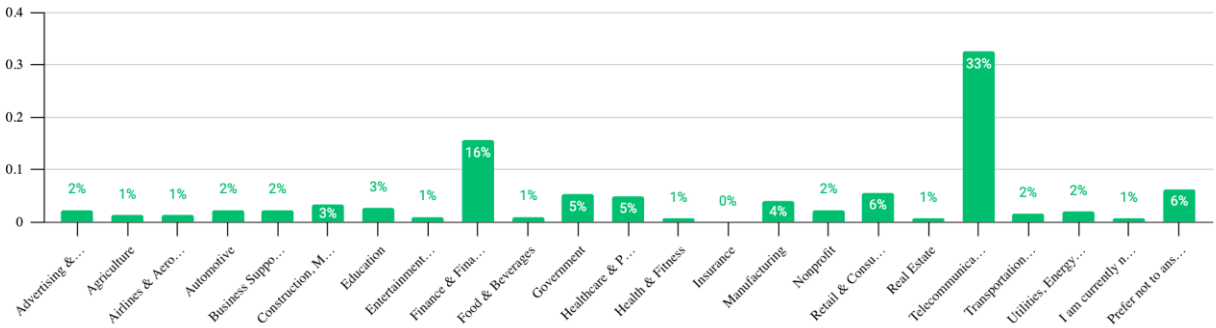
Which best describes your job level?



What is the size of your organization?



Which of the following best describes the principal industry of your organization?



調査方法

Cloud Security Alliance（CSA）は、クラウドコンピューティングと IT 技術におけるベストプラクティスを広く普及させ、サイバーセキュリティを確保することを使命とする非営利団体です。CSA はまた、他のあらゆる形態のコンピューティングにおけるセキュリティの懸念について、これらの業界内のさまざまな利害関係者を教育しています。CSA の会員は、業界の実務者、企業、および専門家団体からなる幅広い連合体です。CSA の主な目標の 1 つは、情報セキュリティの動向を評価する調査の実施です。これらの調査は、情報セキュリティとテクノロジーに関する組織の現在の成熟度、意見、関心、および意向に関する情報を提供します。

Valence Security 社は、SaaS セキュリティに関する業界の知識、態度、および意見をよりよく理解するため、CSA 社に調査とレポートの作成を依頼しました。Valence Security はこのプロジェクトに出資し、CSA の調査アナリストと共同でアンケートを作成しました。調査は 2025 年 1 月に CSA によってオンラインで実施され、さまざまな規模や地域の組織の IT およびセキュリティ専門家から 420 件の回答を得ました。本レポートでは、CSA のリサーチアナリストがデータ分析と解釈を行いました。

調査の目的

本調査の目的は、**SaaS セキュリティの現状を**評価し、重要な課題を明らかにし、企業が SaaS 環境のセキュリティ確保と管理をどのように行っているかを探ることです。業界の洞察を通じて、以下のことを目指します：

- **SaaS のセキュリティ管理に関する理解：**誰が責任を持ち、どのようなツールを使用し、どのようにセキュリティを実施するか。
- **主要なリスクと課題を特定：**設定ミス、アイデンティティ・セキュリティ・ギャップ、シャドー IT、およびサードパーティ・アクセス・リスク。
- **セキュリティ戦略と投資の評価：**SaaS セキュリティの優先順位付け、予算の配分、およびセキュリティソリューションの採用方法。
- **新たな脅威の検証：**AI 主導の統合、SaaS 間接続、および人間以外のアイデンティティ（NHI）の影響。