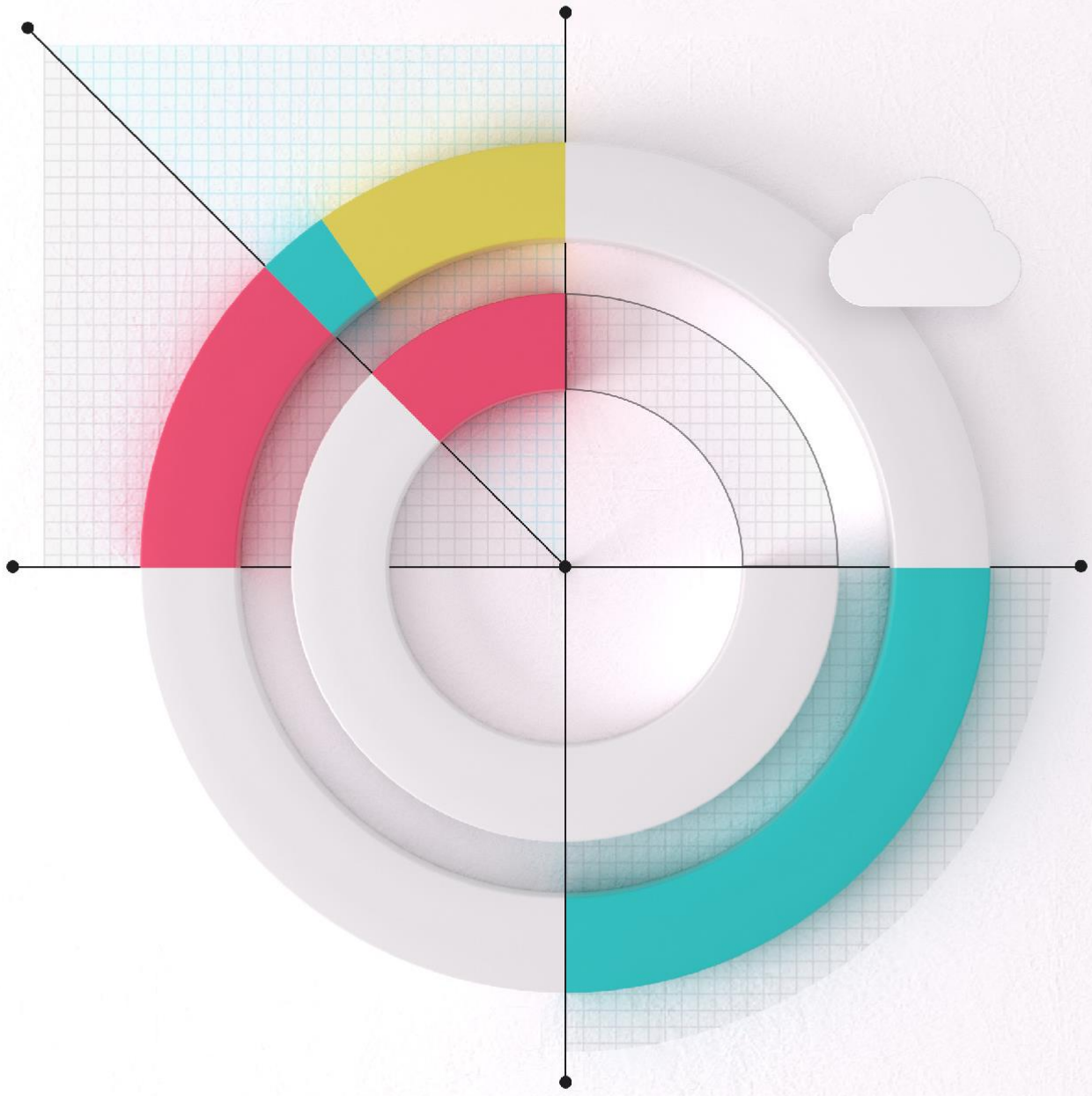
SaaSセキュリティに関する年次調査報告書

2024年　計画と優先順位



日本語版提供に際しての告知及び注意事項

本書「SaaSセキュリティに関する年次調査報告書」は、Cloud Security Alliance (CSA)が公開している「The Annual SaaS Security Survey Report」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
2023年8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

「SaaSセキュリティに関する年次調査報告書」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）

石井　英男
根塚　昭憲
満田　淳
諸角　昌宏

目次

主な調査結果

1 増加するSaaSのセキュリティインシデント

55%の組織が過去2年間にインシデントを経験したと報告しており、さらに12%は不明です。この結果は 、ランサムウェア、マルウェア、データ漏洩など、オンプレミスの一般的な攻撃が、クラウドSaaS環境でも起こりうるという厳しい現実を、企業が理解 しつつあることを示しています。

2 現在のSaaSのセキュリティ戦略や方法論は十分とは言えない

この調査では、半数以上（58%）の組織が、現在のSaaSセキュリティソリューションは、SaaSアプリケーションの50%以下しかカバーしていないと推定していることがわかりました。SaaSのセキュリティインシデントから企業を守るには、手動監査やCASBだけでは不十分であることが明らかになりつつあります。

3 SaaSアプリケーションのセキュリティ確保におけるステークホルダーの広がり

CISOやセキュリティ管理者は、SaaSアプリケーションの所有権が組織のあらゆる部門に分散しているため、コントローラーからガバナーへとシフトしています。組織のSaaSスタックを安全に保護するためには、最適化、コミュニケーション、コラボレーションが重要です。

4 SaaSセキュリティエコシステム全体のポリシーとプロセスを優先させる組織とは？

SaaSセキュリティは、SaaSの誤設定、SaaS間アクセス、デバイスからSaaSへのリスク管理、アイデンティティとアクセスガバナンス、アイデンティティ脅威の検出と対応（ITDR）など、SaaSエコシステムにおける幅広い懸念事項に対応するために適応を続けています。組織は、これらの異なる領域を保護するために必要となる、堅牢なポリシー、プロセス、および機能を導入しています。

5 SaaSへの投資とSaaSのセキュリティリソースが急激に増加

66%の組織がアプリへの投資を増やし、71%がSaaS向けセキュリティツールへの投資を増やしています。具体的には 、SaaS・セキュリティポスチャーマネジメント（SSPM）ソリューションの採用が 大幅に増えており、2022年の17%から2023年には44%に増加したことが示されています。
これは、SSPM が他の手法や戦略ではカバーしきれなかった領域をカバーし、SaaS セキュリティエコシステム全体を通じて様々なセキュリティリスクに対してより包括的な保護を提供することに起因する。

調査票の作成と方法

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と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普及させることを使命とする非営利団体です。また、CSAは、これらの業界内のさまざまな関係者に対して、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教育を行っています。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連合体である。CSAの主要な目的の一つは、情報セキュリティの動向を評価する調査を実施することです。
これらの調査結果は、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、意向に関する情報を提供します。Adaptive Shieldは、SaaSアプリケーションの利用、SaaSセキュリティポリシーとプロセス、SaaSの脅威、SaaSセキュリティ戦略/ソリューションに関する業界の知識、態度、意見をよりよく理解するために、CSAに調査およびレポートの作成を依頼しました。Adaptive Shieldはこのプロジェクトに出資し、CSAのリサーチアナリストと共同でアンケートを作成しました。この調査は、CSAが2023年3月にオンラインで実施したもので、さまざまな規模や場所にある組織のITおよびセキュリティ担当者から1130件の回答を得ました。本報告書のデータ分析および解釈は、CSA のリサーチアナリストが行っています。

研究の目標

本調査の主な目的は、組織におけるSaaSセキュリティのいくつかの重要な側面について深く理解することです。

組織における現在のSaaSアプリケーションの利用状況	SaaSアプリケーションに関する組織のセキュリティポリシーとプロセス	SaaSの脅威に対する認識と経験	セキュリティソリューションの現状と今後の活用

データ&ディスカッション

今日のデジタル環境において、SaaSのセキュリティはあらゆる規模の組織にとって極めて重要です。企業が業務やデータをクラウド、より具体的にはSaaSアプリケーションに移行する機会が増えるにつれ、これらのアプリケーションのセキュリティは最も重要なものとなっています。SaaSアプリケーションは設計上安全ですが、その設定や管理方法こそがリスクとなります。適切なセキュリティ対策を講じなければ、企業はデータ漏洩、サイバー攻撃、その他のセキュリティインシデントにさらされ、大きな財務的・風評的被害を受ける可能性があります。そのため、SaaSのセキュリティを理解することは、企業がこれらのリスクから身を守るために必要不可欠です。

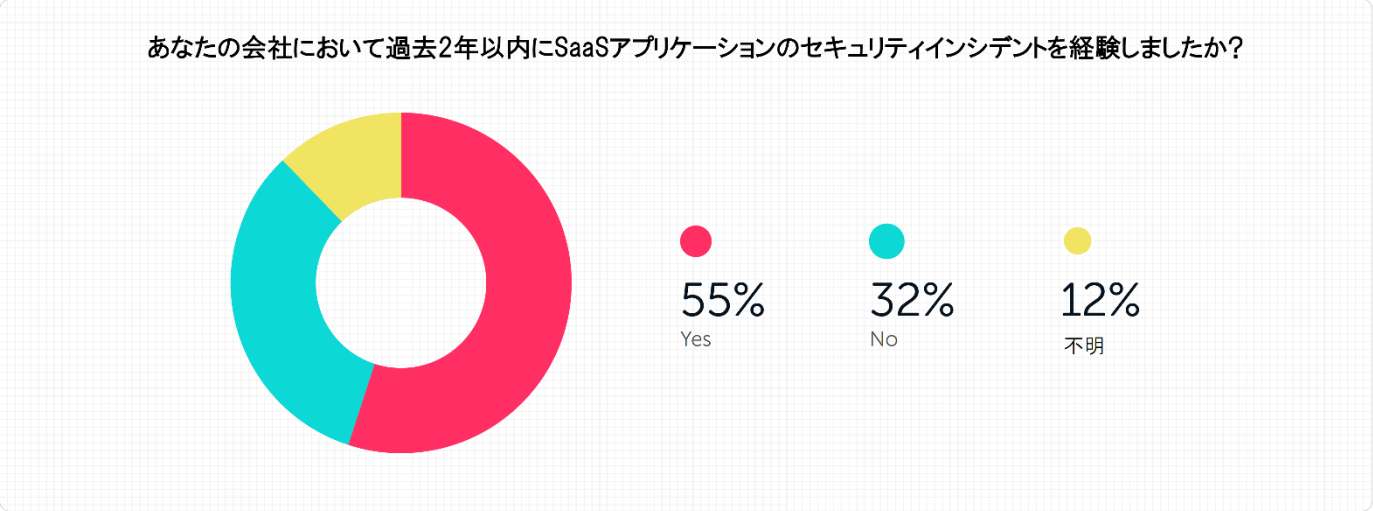
このような背景から、本調査では、昨年に引き続き、SaaSセキュリティの複雑な実態に迫ります。以下、今年の調査結果と考察をご紹介します。

キーファインディング#1

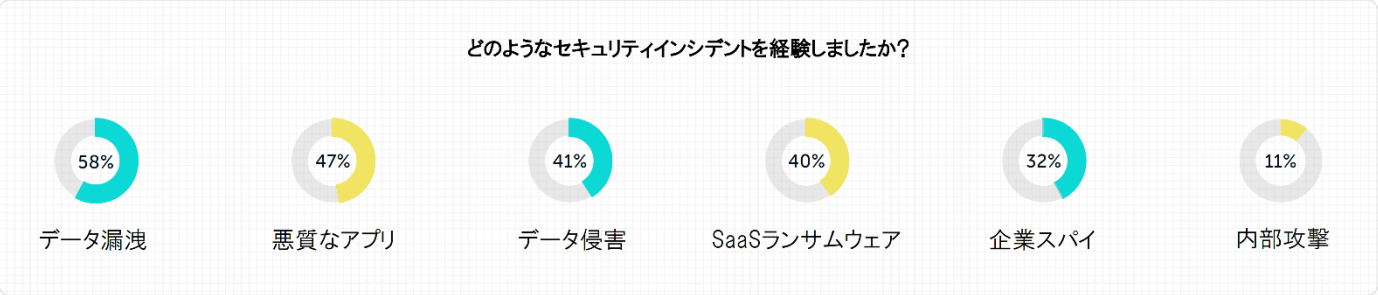
増加するSaaSのセキュリティインシデント

この調査では、SaaSエコシステム内でのセキュリティインシデントが大幅に増加していることが明らかになり、過去2年間にインシデントを経験したと回答した組織は55%で、前年から12%増加しました。約3分の1（32%）の回答者は、同期間内にSaaSのセキュリティインシデントに遭遇していないと回答し、12%は不明と回答しています。

この調査結果は、ランサムウェア、マルウェア、データ漏洩など、オンプレミスの一般的な攻撃がSaaS環境でも発生しうるという厳しい現実を、多くの企業が認識しつつあることを物語っています。



最も多く報告されたSaaSセキュリティインシデントは、データ漏洩（58%）、悪意のあるアプリ（47%）、データ侵害（41%）、SaaSランサムウェア（40%）で、堅牢なセキュリティ対策の必要性の高まりとSaaS環境の拡大に伴う潜在リスクへの認識の高まりが浮き彫りになっています。

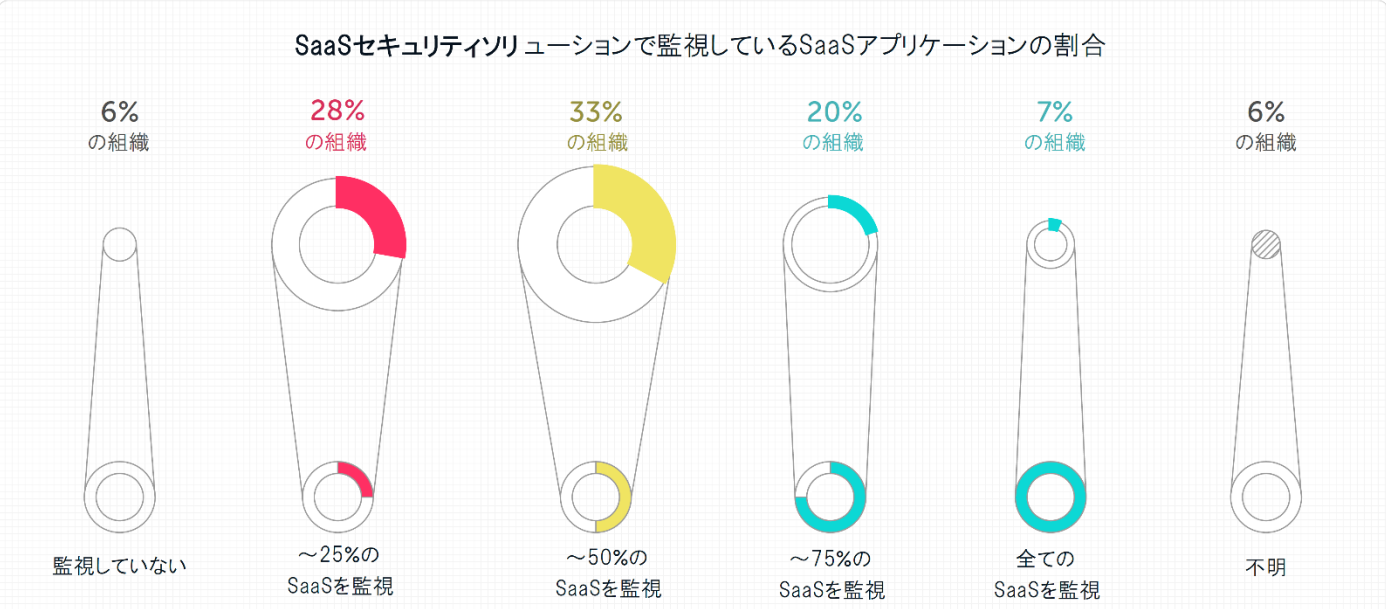


キーファインディング#2

現在のSaaSのセキュリティ戦略と方法論は、十分に行き届いていない

SaaSアプリケーションの監視が十分でない

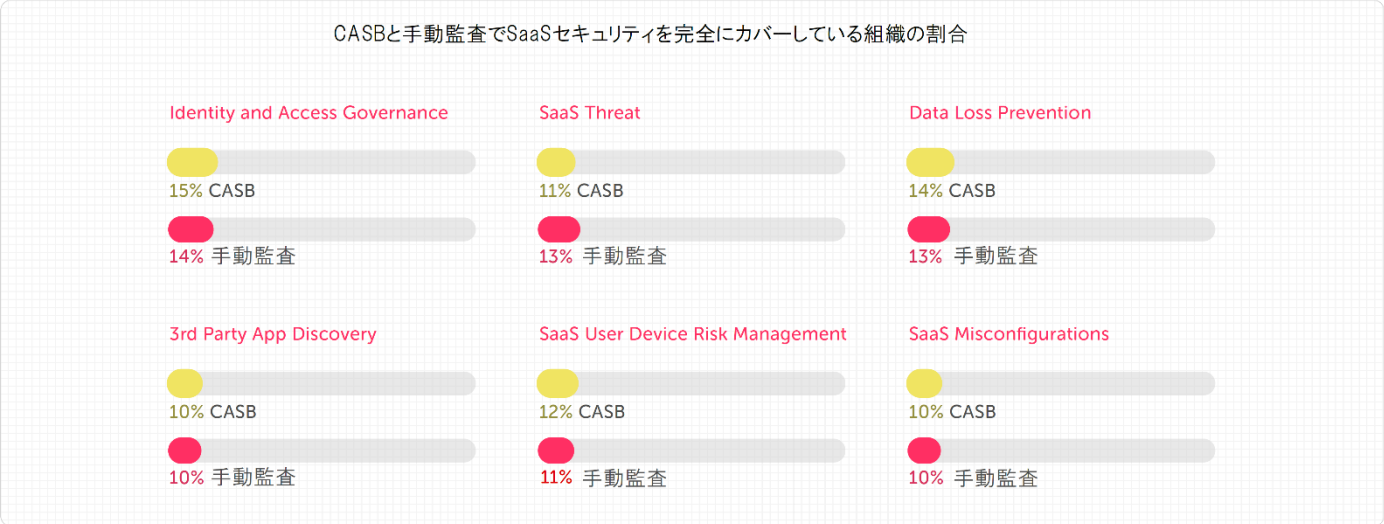
調査結果からは、効果的なSaaSセキュリティ対策の実施に関して、かなりの数の組織が不十分であることが示唆されており、それがSaaSセキュリティインシデントの増加につながっている要因の1つであると言えます。多くの企業は、SaaSスタック全体をカバーしないセキュリティソリューションを使用しており、アプリケーションやデータがサイバー脅威にさらされたままになっています。具体的には、半数以上（58%）の組織が、現在のSaaSセキュリティソリューションは、SaaSアプリケーションの50%以下しかカバーしていないと推定していることがわかりました。



これらの結果は、企業が自社のセキュリティソリューションを再評価し、SaaSエコシステム全体を包括的にカバーできるようにすることが急務であることを強調しています。そうすることで、企業はデータ漏洩、ランサムウェア攻撃、その他の種類のサイバー攻撃を含むセキュリティインシデントのリスクを大幅に低減することができます。そのことが、最終的には、自社の評判を守り、顧客の信頼を維持することにつながるのです。

SaaSのセキュリティには、CASBと手動監査が不足している

多くの企業は、SaaSアプリケーションのセキュリティを確保するために、クラウドアクセスセキュリティブローカー（CASB）と手動監査に頼っています。しかし、これらの方法は、いくつかの重要な分野で不十分であることが判明しています。さらに、手作業による監査では、監査と次の監査までの間に会社のデータが流出する可能性があるため、その間はセキュリティインシデントのリスクが発生します。



これらの調査結果は、企業がセキュリティ戦略を再評価し、セキュリティインシデントのリスクを低減するために、 SaaSエコシステム全体をカバーする、より包括的なソリューションと戦略に投資する必要があることを示しています。また、SaaS型セキュリティポスチャーマネジメント（SSPM）ツールの利用が増加しているのも、このような背景があると思われます。

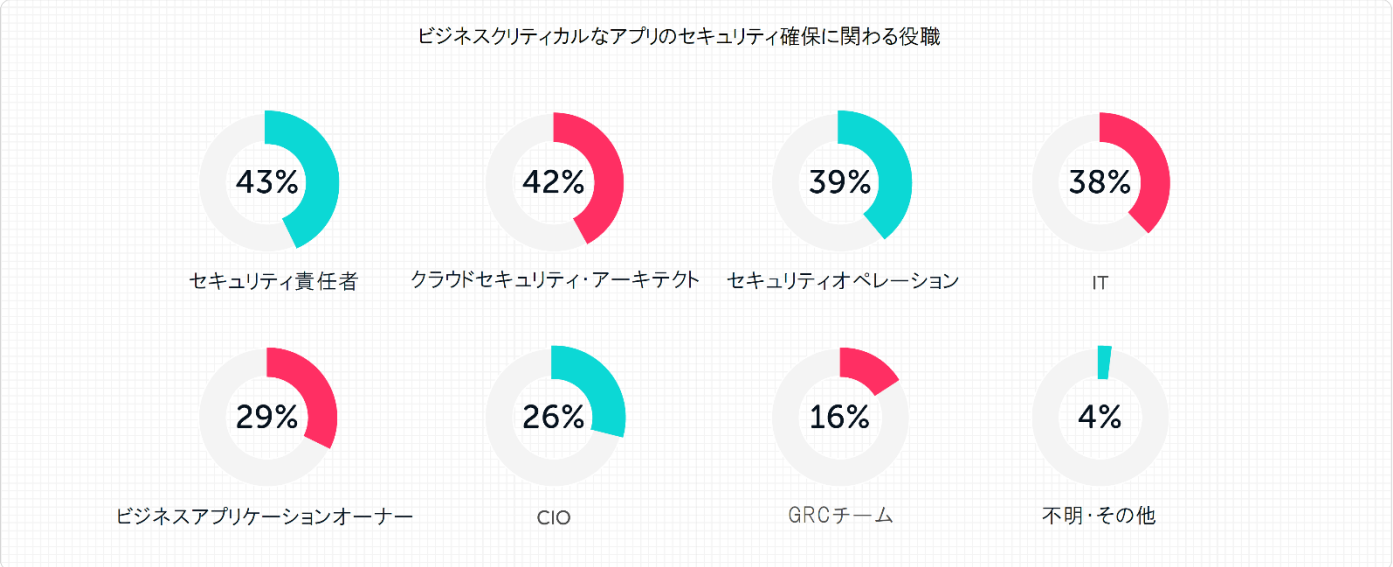
キーファインディング #3

SaaS アプリケーションのセキュリティ確保におけるステークホルダーの広がり

ツール、セキュリティ、スタッフへの金銭的な投資に加え、企業はビジネスクリティカルなアプリケーションを保護するプロセスにおいて、多くの利害関係者を巻き込むようになってきています。一般的な組織では、ファイル共有やコラボレーションアプリから、CRM、プロジェクトや仕事の管理、マーケティングオートメーションなど、さまざまなSaaSアプリが利用されています。SaaSアプリは様々なニッチな役割を担っていますが、このステークホルダーの広がりは脅威の状況を複雑にしています。

現在、CISOやセキュリティ管理者は、SaaSアプリのセキュリティを管理する立場から統治する立場へと移行しつつあり、今回の調査では、セキュリティガバナンスに携わる人のうち、幹部クラスの役職や部門長を務める人がいかに多いかを示しており、企業がSaaSセキュリティに真剣に取り組んでいることを示しています。重要な意思決定者が参加したことで、SaaSセキュリティが貴重な資産を保護し、事業継続を確保する上で重要な役割を果たすという認識が高まっていることが強調されました。

しかし、多くの人が関わっているため、誰がSaaSセキュリティの最終的な責任を負うのかを判断することは困難となります。SaaSアプリケーションは、セキュリティチームがSaaSアプリケーションに直接アクセスできるとは限らないため、セキュリティチームとアプリ所有者の間で緊密な連携を多く必要とします。そのため、SaaSのセキュリティ管理を効果的に行うために不可欠なアプリの所有者を積極的に巻き込み、ギャップを埋めることができるプロセスやツールが必要です。



コラボレーション環境を醸成し、セキュリティチームとアプリ所有者の間のコミュニケーションと調整を促進するソリューションや戦略を導入することで、企業はビジネスクリティカルなアプリケーションを保護するために、より堅牢で合理的なアプローチを構築できます。これにより、潜在的な脅威を最小限に抑え、進化し続けるSaaSのセキュリティ脅威に対してより高いレベルの保護を実現することができます。

キーファインディング #4

組織が SaaS セキュリティ エコシステム全体のポリシーとプロセスに優先順位を付ける方法 とは？

過去1年間、ビジネスクリティカルなSaaSアプリケーションへの投資の増加、セキュリティインシデントの増加、SaaSアプリケーションを標的とする脅威者の増加などの要因により、SaaSセキュリティの焦点は大きく進化しています。以前は、組織やSSPMのようなセキュリティツールは、誤設定管理に主眼が置かれていました。しかし、SaaSセキュリティは、SaaS間アクセス、デバイス間リスク管理、アイデンティティとアクセスガバナンス、アイデンティティ脅威検出と応答（ITDR）など、より幅広い懸念事項を包含するように適応しています。

ポリシー・プロシージャの策定

ビジネスシーンにおけるSaaSの重要性が高まる中、組織のSaaSスタックとその中に含まれるデータを脅威から保護するためには、強固なポリシー、プロセス、および機能を導入することが不可欠です。

組織は現在、主要分野に対処するための対策を講じています。以下のデータは、SaaSセキュリティエコシステムのさまざまなドメインを通じて、SaaSスタックのセキュリティを確保する際に、組織が何を優先し始めているかを示すものです。

コンフィギュレーション管理

組織のSaaSスタックを、脅威アクターに悪用される可能性のある誤ったセキュリティ設定から保護するためには、設定ミスの問題に対処することが重要です。回答者の設定ミス管理の優先順位は、主に以下の通りです：

セキュリティチームとアプリオーナーチーム間のコミュニケーションとコラボレーション	詳細な修正と設定ミスの緩和	アプリケーション、セキュリティドメイン、リスクレベルに基づく優先順位付け

強力なシステムとプロセスを導入することで、これらの影響度の高い領域は、SaaSの攻撃対象領域を縮小することができます。

サードパーティアプリのアクセス

サードパーティのSaaSアプリケーション（コアスタックに接続するアプリケーション）への依存度が高まる中、潜在的なリスクを評価し管理するためのポリシーが極めて重要になっています。サードパーティアプリのアクセスに関する主な優先順位は以下の通りです：

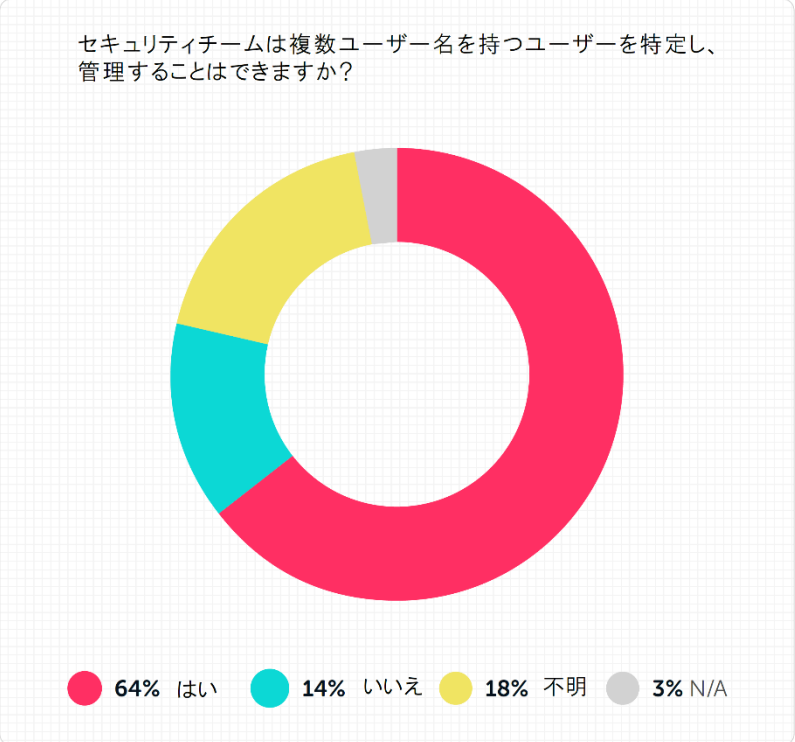
接続されたサードパーティ製SaaSアプリケーションのリスクを検索、検出、定量化する。	SaaSスタックに統合された悪意のあるアプリを検出する	アプリの所有者がアプリを接続する前に、セキュリティへのリクエストを提出することを要求するプロセス

これらの優先順位は、サードパーティ製アプリへのアクセス脅威から保護するための強力なシステムとプロセスの必要性を反映しています。

SaaS アイデンティティ&アクセスガバナンス

SaaSエコシステム内の機密データを保護するためには、適切なアイデンティティとアクセスガバナンスが不可欠です。今日、組織におけるアイデンティティとアクセスガバナンスの優先課題は以下の通りです：

- 各ユーザーが必要なレベルのアクセス権を持つようにする
- Active Directoryで無効化されているにもかかわらず、SaaSアプリケーションにアクセスできるユーザーを検出することができます。
- 休眠アカウントを検出し、必要に応じてSaaSへのアクセスのデプロビジョニングを迅速に行う。
- 管理者アクセス権の通知
- 認証の実践（例：鍵管理、証明書管理）



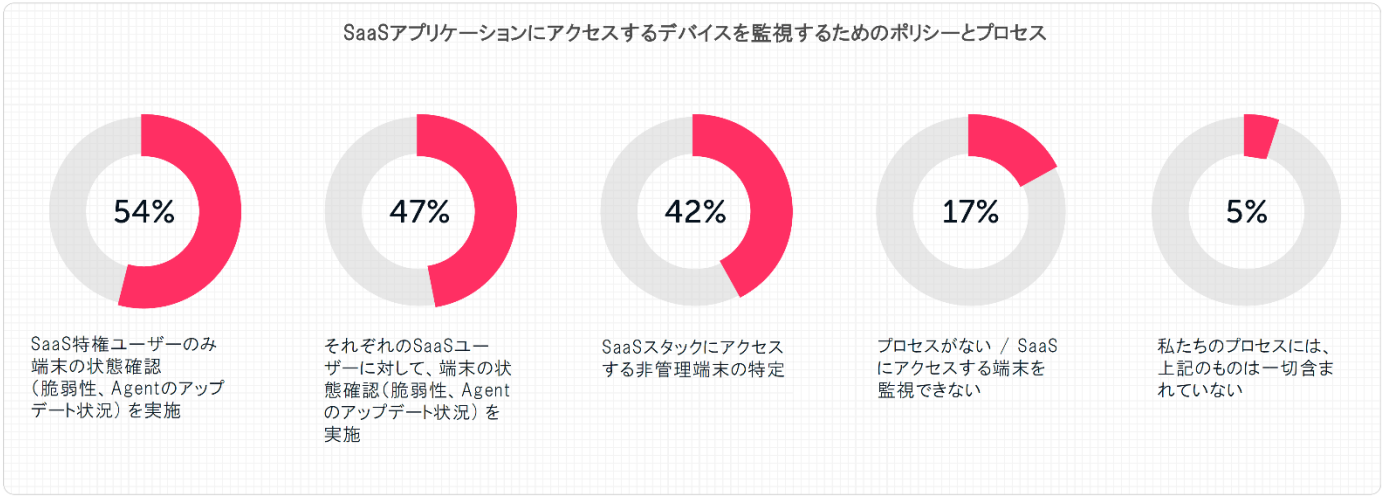
SaaSユーザーデバイスの監視

SaaSスタックにアクセスするデバイスのセキュリティを確保することは、不正アクセスやデータ漏洩を防止するために重要です。SaaSのリスクがデバイスに起因するものでないことを確認するための組織の優先順位は以下の通りです：

特に特権を持つSaaSユーザー一人ひとりのデバイスの衛生状態（脆弱性、更新されたエージェント）をチェックする。

SaaSスタックにアクセスする管理されていないデバイスを特定する。

多くの人は、デバイスをSaaSアプリのセキュリティの弱点と見なしていません。デバイスはゲートウェイであり、特権ユーザーのデバイスが安全でない場合、脅威アクターが成功した場合の損害は甚大となるでしょう。



脅威の検知と対応

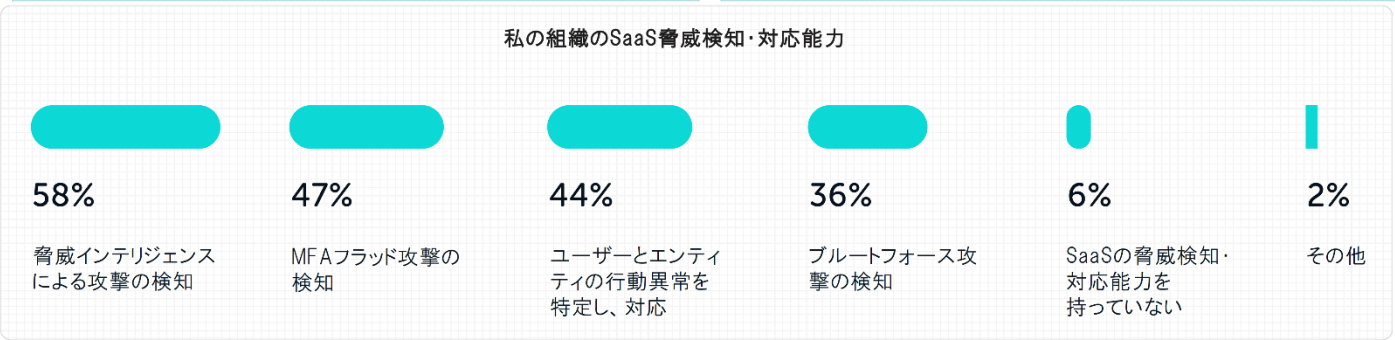
標的型攻撃から組織を守るためには、プロアクティブな脅威の検知と対応が重要です。今日の環境における、脅威の検出と対応の優先順位は、次のとおりです：

ユーザーやエンティティの行動異常の特定と対応

MFAフラッドアタックを検知する

脅威インテリジェンスで攻撃を検知する

ブルートフォースアタックを検知する



キーファインディング#5

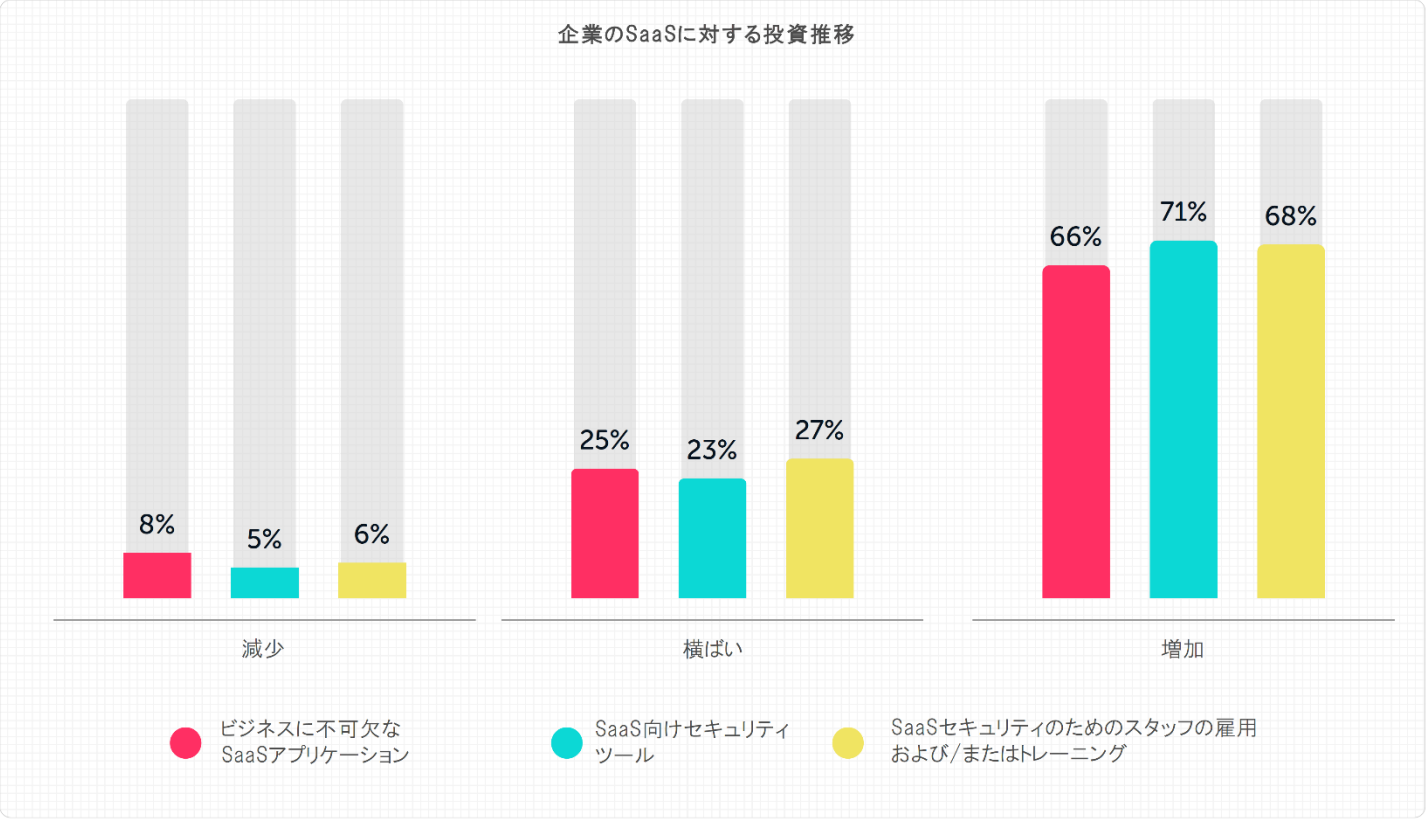
SaaSへの投資とSaaSのセキュリティリソースが激増

SaaSへの投資の増加

組織は、ビジネスに不可欠なアプリやスタッフだけでなく、SaaSセキュリティに焦点を当てた適切なセキュリティツールも含め、SaaSリソースへの依存度を高めています。

調査によると、71%の組織がSaaS向けセキュリティツールへの投資を増やしており、デジタル資産の保護に向けた取り組みが進んでいることがわかります。さらに、68%の企業が、SaaSセキュリティに関するスタッフの雇用とトレーニングへの投資を強化しており、SaaSエコシステムを保護するための人的資本の重要性を認識しています。さらに、66%の企業がビジネスクリティカルなSaaSアプリケーションへの投資を増加させており、これはコアビジネス機能におけるこれらのツールへの依存度の高まりを反映しています。

このように、セキュリティツール、人材、アプリケーションを包括したSaaSへの投資は、SSPMのような強固なセキュリティソリューションの重要性を際立たせています。



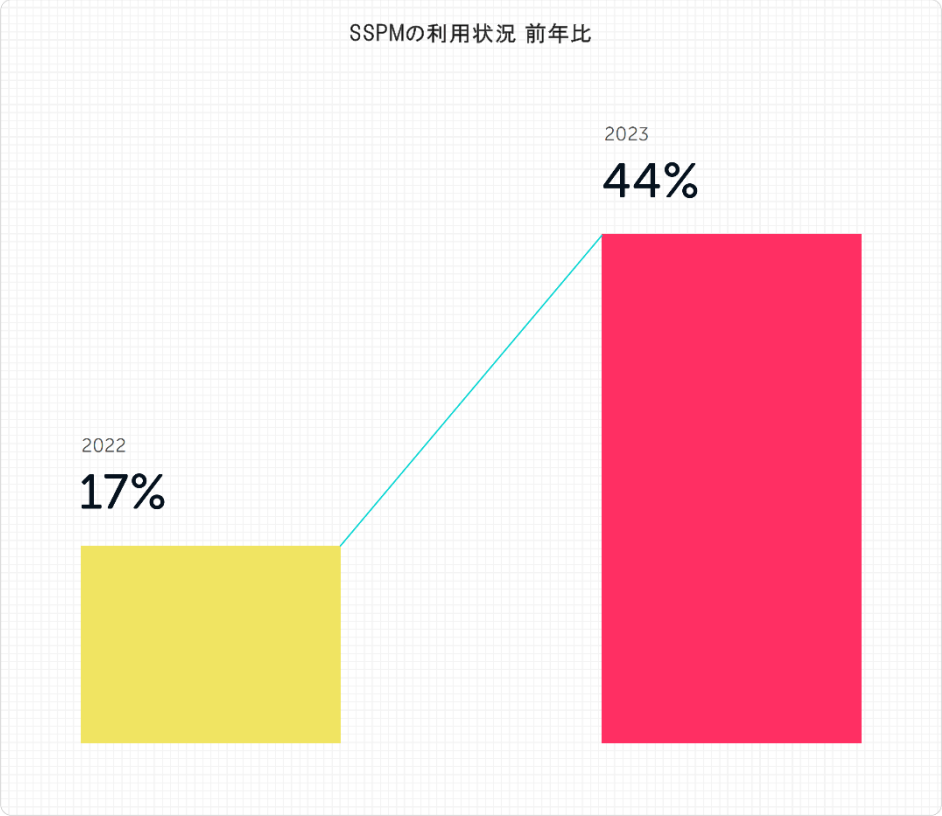
SaaS型セキュリティポスチャーマネジメント（SSPM）の利用増加

SaaSセキュリティインシデントが増加し、現行のSaaSセキュリティ手法（CASBや手動監査など）では不十分なため、組織はSSPMのようなより高度なSaaSセキュリティツールを求めています。この調査によると、SSPMツールの採用率は大幅に増加しており、2022年に17%だったSSPMを利用している組織の割合は、2023年には44%に増加しています。

これは、SSPMが他の手法や戦略ではカバーしきれなかった領域をカバーし、SaaSセキュリティエコシステム全体を通して様々なセキュリティリスクに対してより包括的な保護を提供することに起因していると思われます。

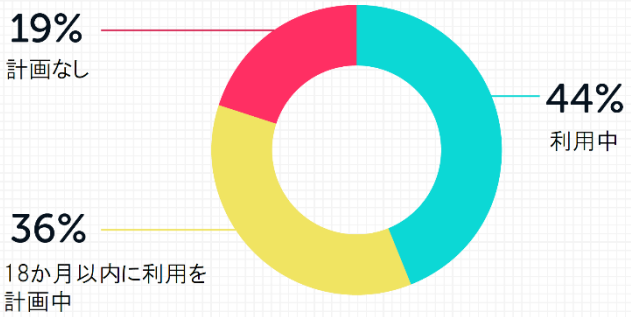
本紙の冒頭でも紹介しましたが、ここで要約すると、次のような領域が含まれます。

- **SaaSの誤設定**：SaaSアプリケーションの適切な設定を確保し、侵害を回避する。
- **アイデンティティとアクセスガバナンス**：SaaSアプリケーションやリソースへのユーザーアクセスを管理・制御する。
- **サードパーティアプリのアクセス**：SaaS環境にアクセスするサードパーティアプリケーションに関連するリスクを特定し、管理する。
- **データ損失管理**：SaaSアプリケーションにおける機密データの損失や漏えいを防止・軽減する。
- **接続された悪意のあるアプリ**：SaaS環境のセキュリティを脅かす可能性のある悪意のあるアプリケーションを検出・削除する。
- **脅威の検出と対応**：リアルタイムでセキュリティ脅威をプロアクティブに特定し、対応する。
- **SaaS ユーザーデバイス**：SaaSアプリケーションに接続するユーザーデバイスに関連するセキュリティリスクを監視・管理する。



SaaSのセキュリティインシデントが増え続ける中、組織はSaaSCASBや手動監査といった他のセキュリティ手法の限界を認識しつつあります。SSPMソリューションの導入が増加していること、および導入を計画している企組織の割合が高いことは、進化し続けるSaaSのセキュリティ脅威から保護するために、より堅牢で包括的なセキュリティ対策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。

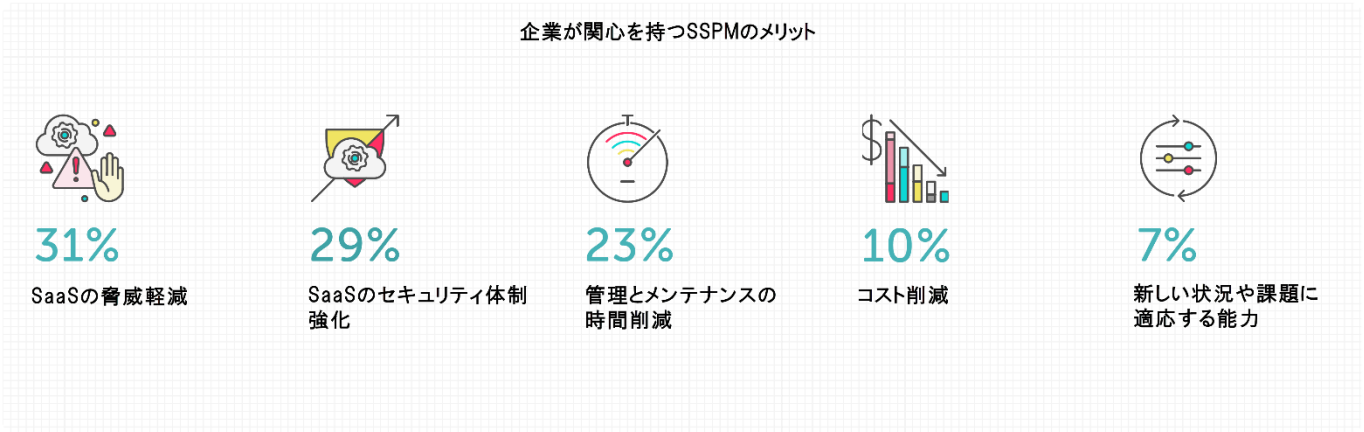
現在、SaaSセキュリティ管理（SSPM）プラットフォームを利用しているか、または利用を計画していますか？



SSPMのメリット

SaaSセキュリティの重要性が高まる中、より包括的で強固なアプローチが必要であることは明らかである。SSPMのようなSaaSセキュリティツールは、今日のSaaSセキュリティ環境に必要なポリシー、プロセス、機能で組織を支援することができます。これらの重要な側面に焦点を当てることで、組織は貴重な資産をよりよく保護し、複雑化する脅威の状況下でビジネスに不可欠なアプリケーションの安全な運用を確保することができます。

企業が関心を持つSSPMのメリット



組織は、SaaS環境における進化する課題に対処するために、SSPMのようなSaaSセキュリティツールを採用することの価値をますます認識するようになっています。このことは、過去1年間に44%がすでにSSPMソリューションを採用し、36%が今後18ヶ月以内にSSPMを採用する予定であることを物語っています。これらのツールを活用することで、企業はSaaSの脅威を効果的に軽減し、全体的なセキュリティ態勢を大幅に強化することができます。

さらに、SSPMを利用することで、従来は手作業で行っていた様々なセキュリティプロセスを合理化・自動化し、管理・保守にかかる時間を短縮することが可能です。この自動化は、手作業の必要性を減らすことでコスト削減につながるだけでなく、組織が他の重要な分野にリソースを再配分することを可能にします。さらに、SaaS型セキュリティツールは、新たな状況や新たな脅威に対応するために必要な適応性を備えているため、組織は常に変化する環境の中でデジタル資産や重要なアプリケーションを保護するための機敏な対応と準備を維持することができます。

デモグラフィック

この調査は、CSAが2023年3月にオンラインで実施したもので、さまざまな規模や場所にある組織のITおよびセキュリティ担当者から1130件の回答を得ました。

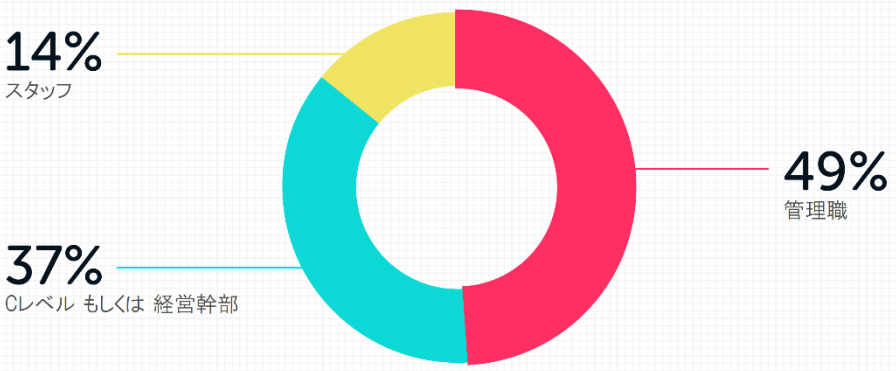
どのような業界で働いていますか？

17% テクノロジー	11% 金融サービス	6% 政府機関	6% プロフェッショナルサービス（法律、コンサルティングなど）	6% メディア
5% ヘルスケア	5% 教育	5% 保険	5% Eコマース、小売り	5% エネルギー、公共事業
5% フード	5% 工業（製造業、建設など）	4% 製薬	3% 銀行業	3% 輸送・ロジスティクス
3% 公益事業	2% 電気通信	1% 農業・鉱業	1% その他	1% 旅行・ホスピタリティ

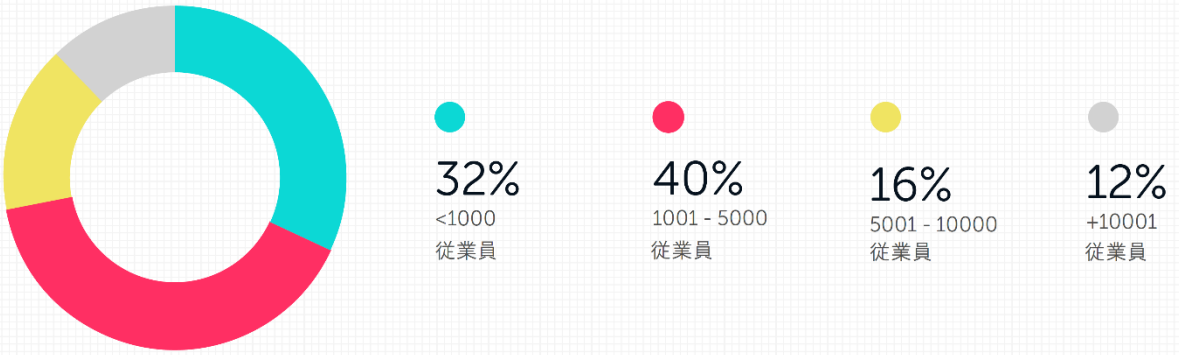
次のうち、あなたの役割に最も近いものは？

18% IT	12% サイバーセキュリティ	9% クラウドセキュリティアーキテクト	8% SaaSセキュリティ	7% 副CISO	7% 情報セキュリティ
7% クラウドセキュリティ	5% GRC	4% SaaSセキュリティアーキテクト	4% CISO	3% セキュリティ技術者	2% CIO
2% セキュリティオペレーション	2% フォレンジック専門家	2% ベンダーリスク評価	2% ペネトレーションテスター	1% 脆弱性管理	5% その他

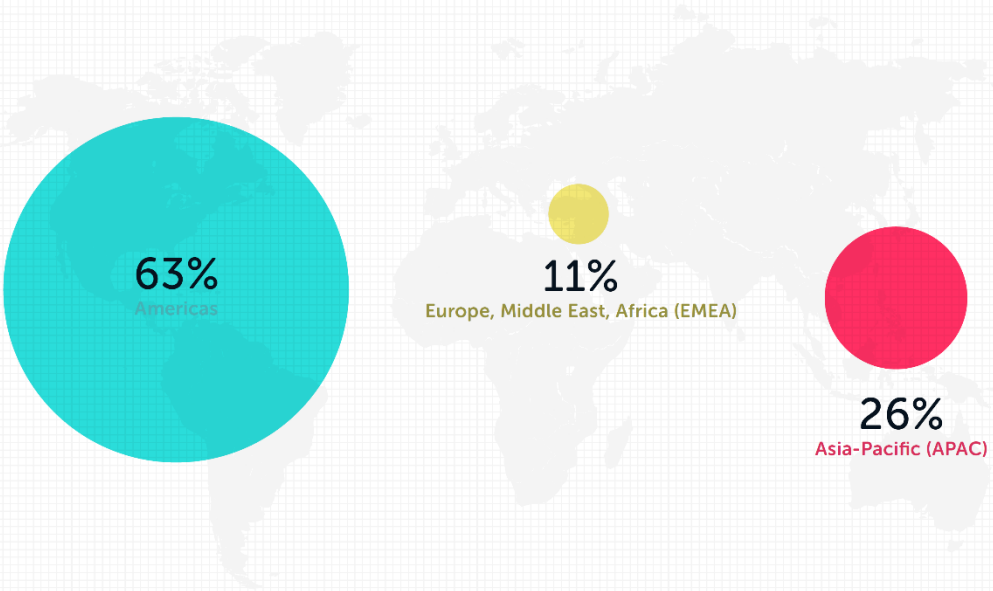
あなたの職務レベルは？



組織の規模は？

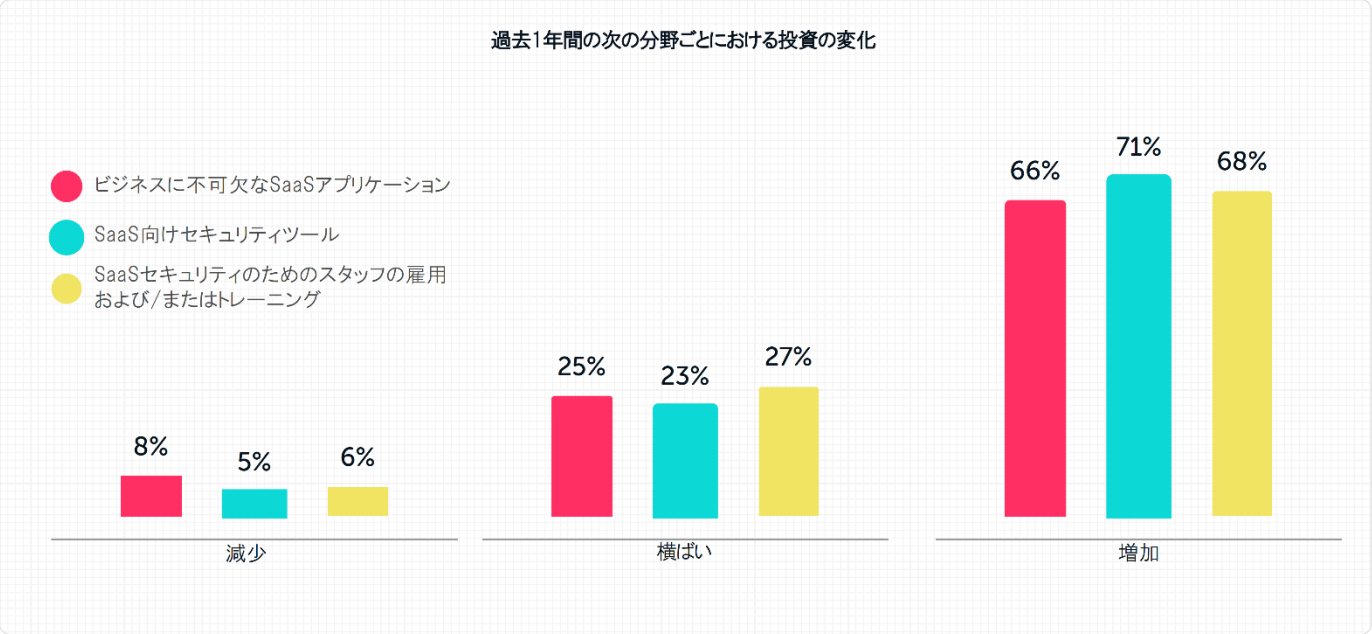


世界のどの地域にお住まいですか？

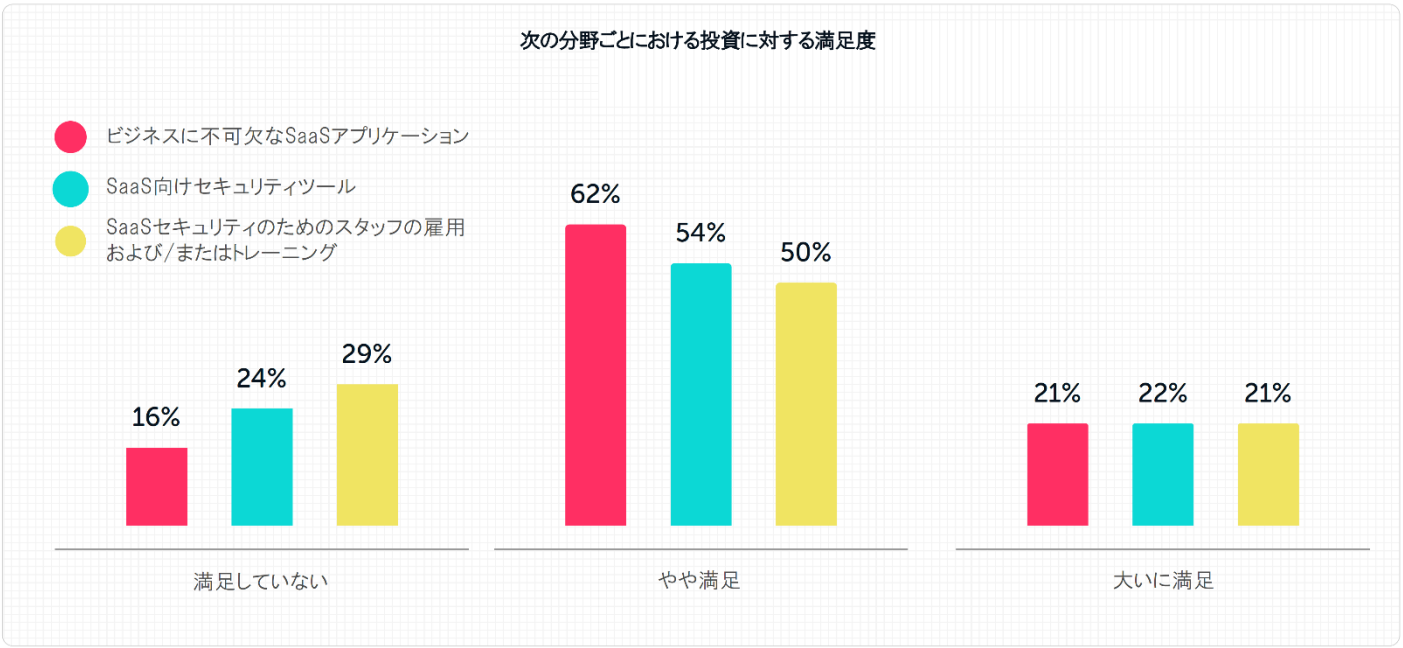


付録A: アンケート結果

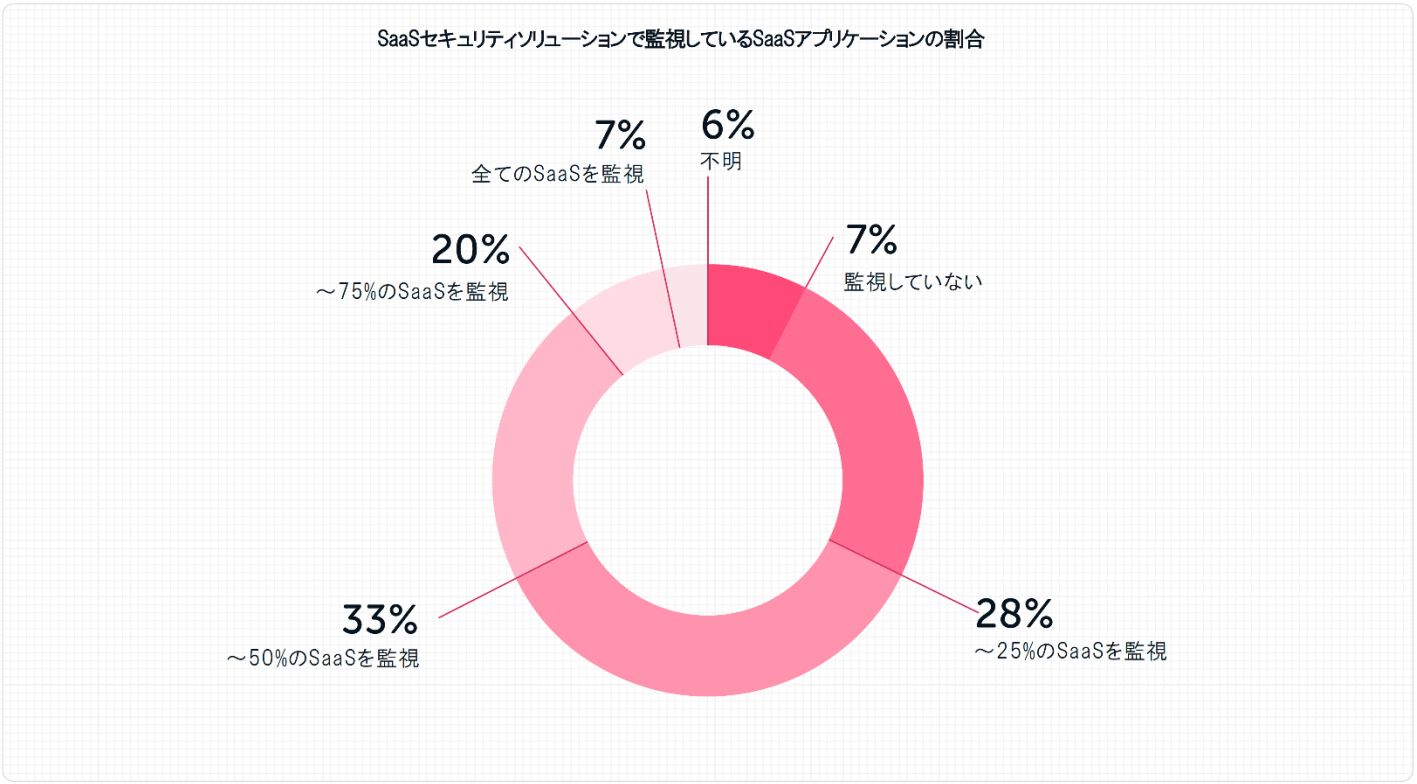
企業のSaaS投資額の推移



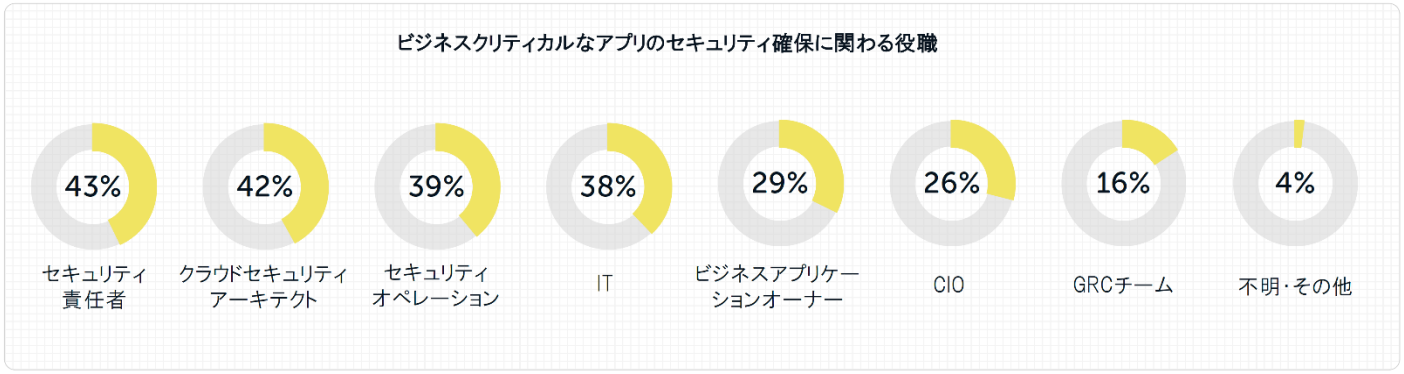
企業のSaaSへの投資に対する満足度



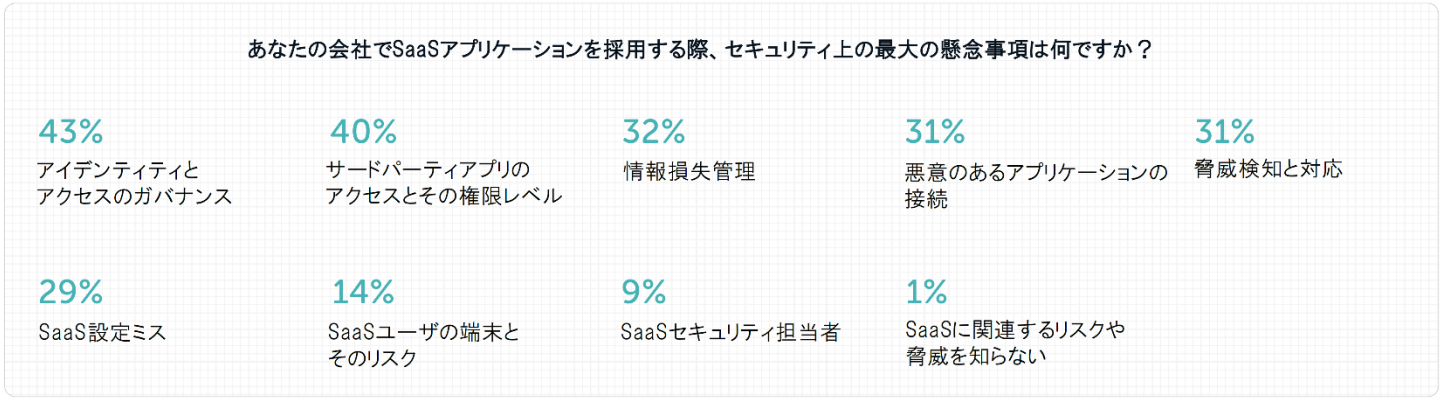
SaaSセキュリティソリューションで監視している SaaSアプリケーションの 割合



ビジネスクリティカルなアプリケーションのセキュアにする職務



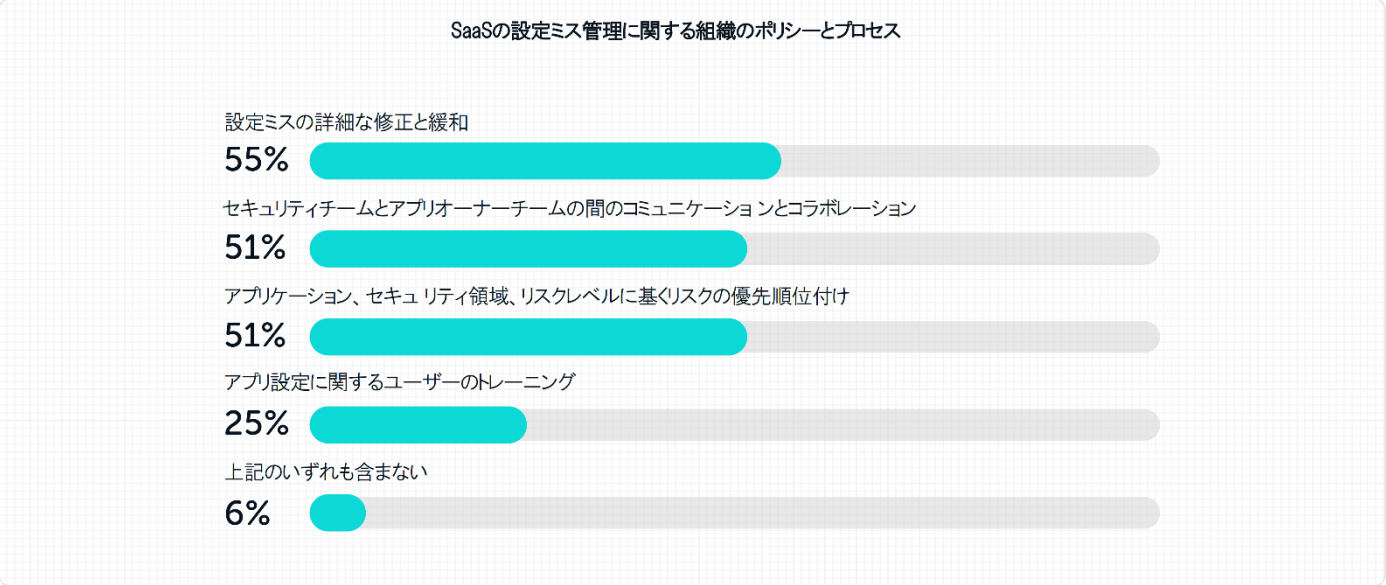
セキュリティに関する主な懸念事項



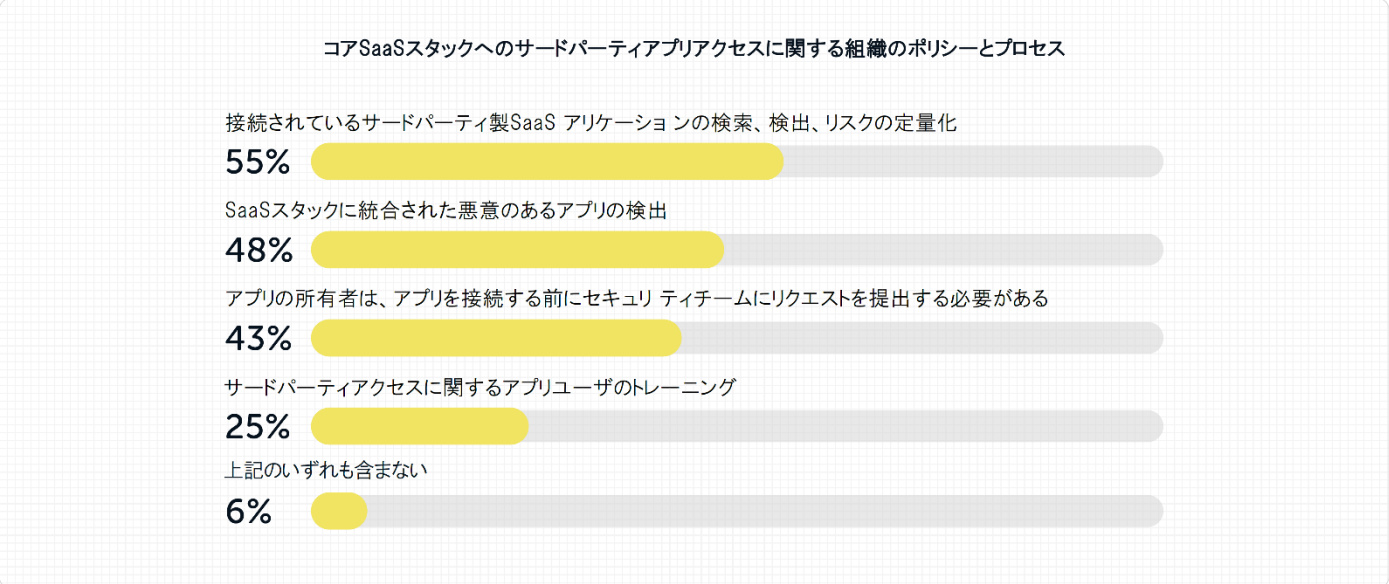
SaaSのセキュリティポリシーとプロセス

このセクションでは、該当する回答をすべて選んでいただきました。

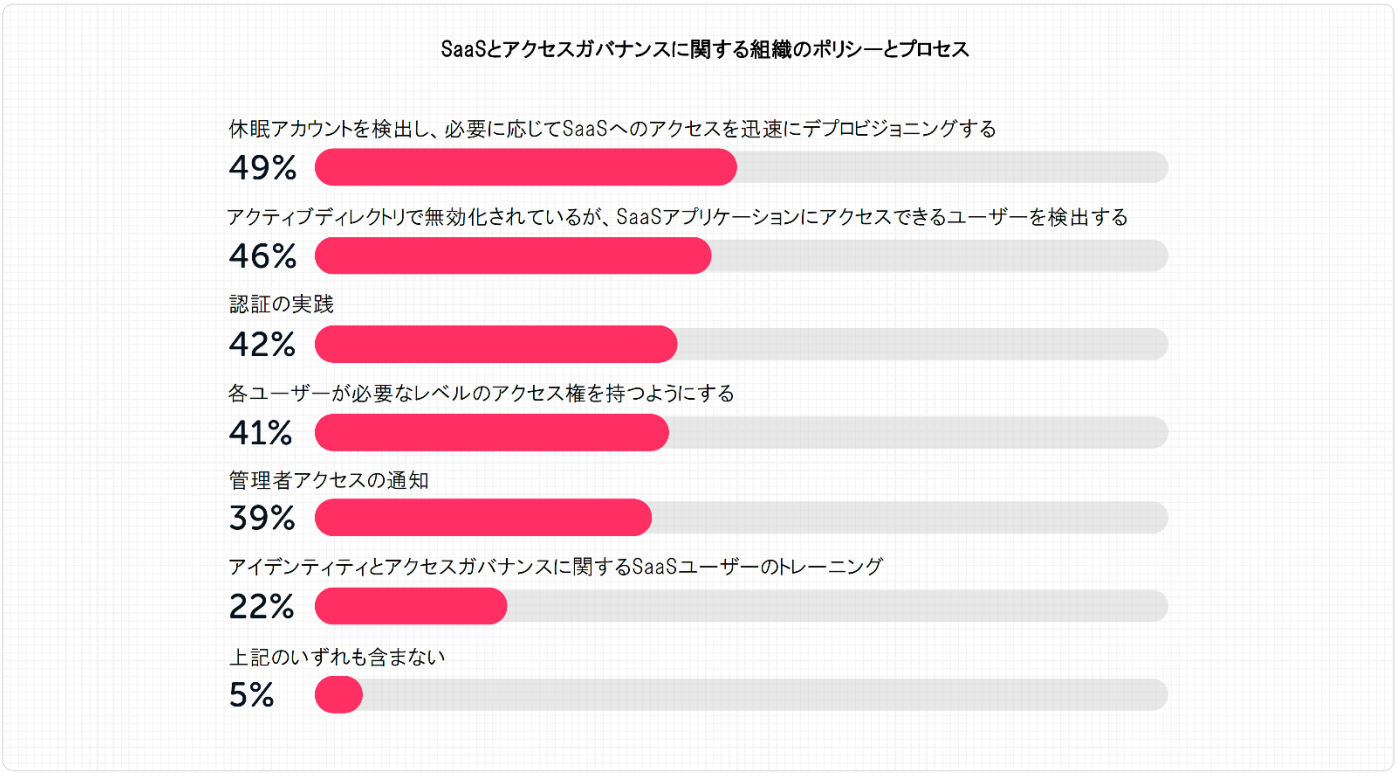
設定ミスの管理

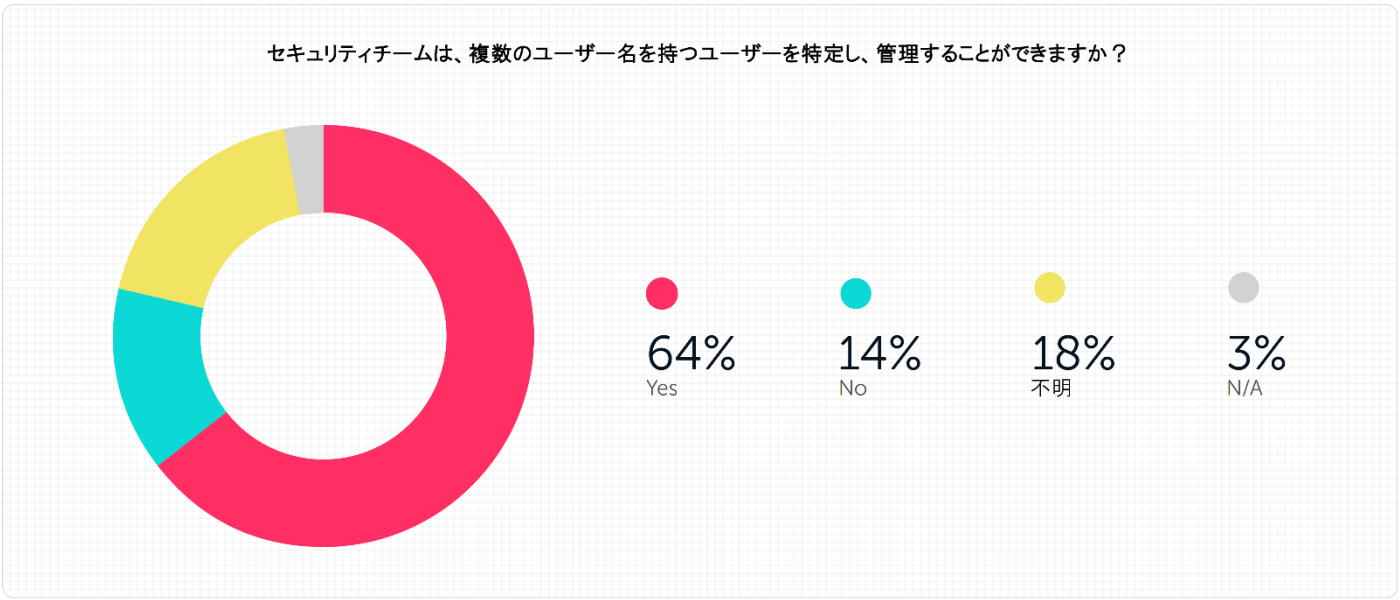


コアなSaaSスタックへアクセスするサードパーティアプリケーション



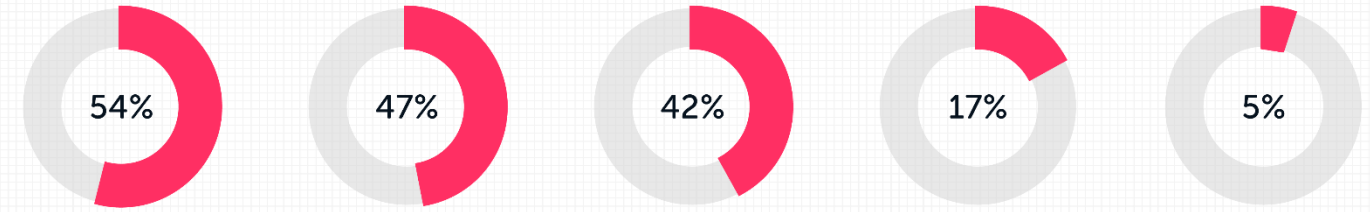
アイデンティティとアクセスガバナンス





SaaSアプリケーションにアクセスするデバイスの監視

SaaSアプリケーションにアクセスするデバイスを監視するためのポリシーとプロセス



- 54% SaaS特権ユーザーのみ端末の状態確認（脆弱性、Agentのアップデート状況）を実施
- 47% それぞれのSaaSユーザーに対して、端末の状態確認（脆弱性、Agentのアップデート状況）を実施
- 42% SaaSスタックにアクセスする非管理端末の特定
- 17% プロセスがない / SaaSにアクセスする端末を監視できない
- 5% 私たちのプロセスには、上記のものは一切含まれていない

SaaSの脅威に対する検知・対応能力

組織のSaaS脅威検知・対応能力

- 58% 脅威インテリジェンスによる攻撃の検知
- 47% MFAフラッド攻撃の検知
- 44% ユーザーとエンティティの行動異常を特定し、対応
- 36% ブルートフォース攻撃の検知
- 6% SaaSの脅威検知・対応能力を持っていない
- 2% その他

SaaSのセキュリティに関するデータ損失防止

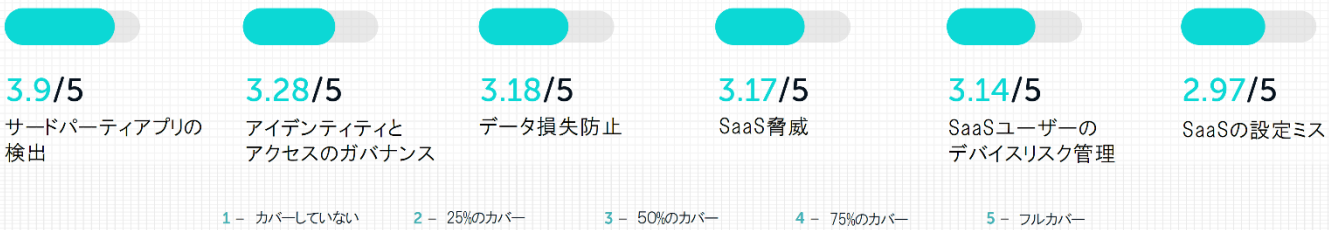
SaaS セキュリティに関するデータ損失防止（DLP）のポリシーとプロセスに含めていること

- 51% グループまたは役割ごとにデータアクセスを制限するポリシーを確立
- 44% 過剰なデータダウンロードに対する警告
- 42% 外部共有データのパスワード保護
- 34% データへの過度なアクセスに対する警告
- 28% 外部共有データへのアクセス有効期限
- 2% SaaS DLPのトレーニング

SaaSの脅威

SaaSに対するCASBのカバレッジ

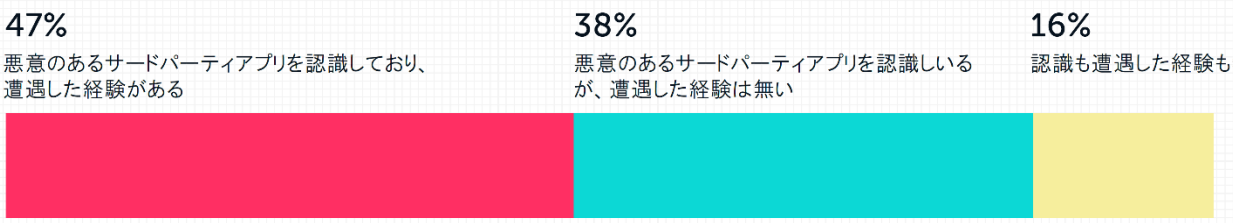
SaaSのセキュリティ確保にCASBを使用している場合、このソリューションから以下の領域でどの程度のカバレッジを得ていますか？



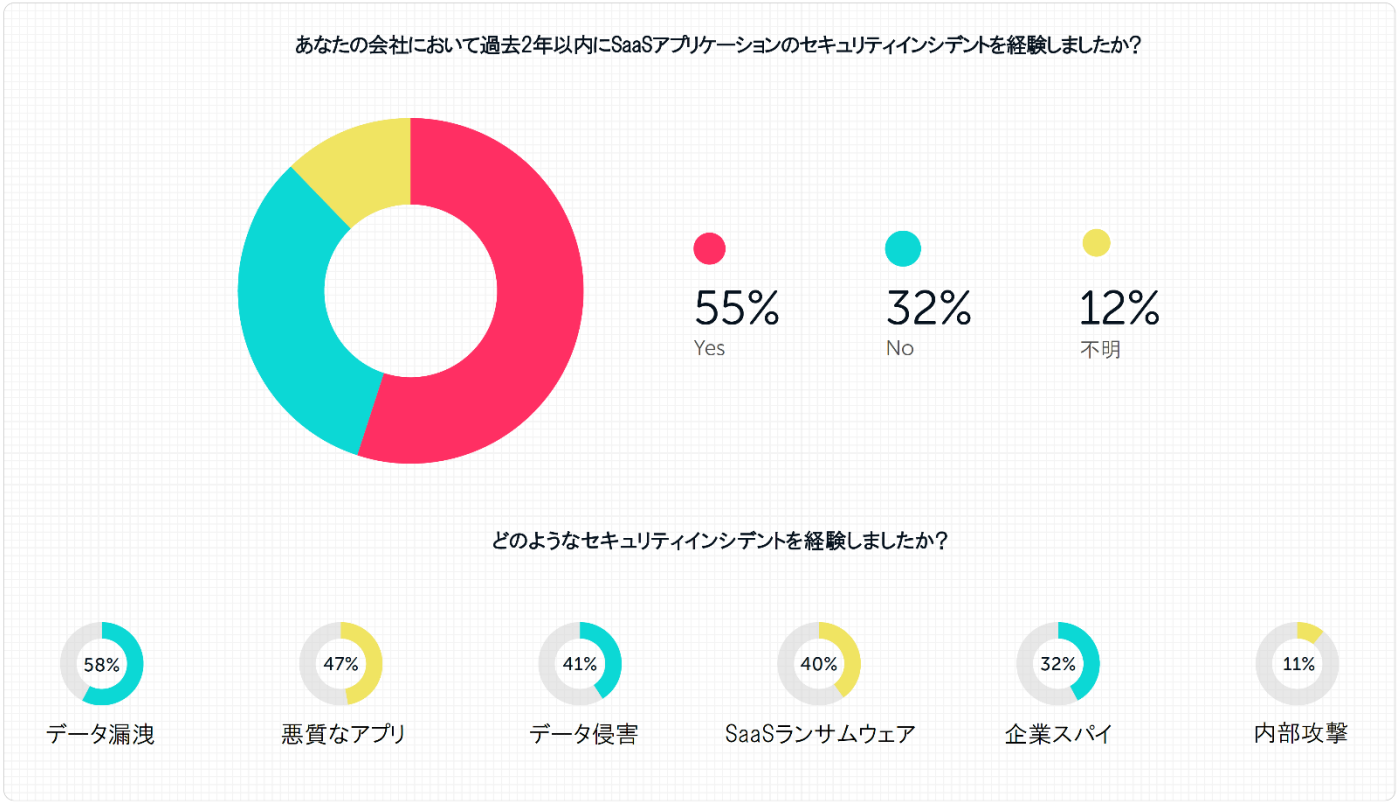
SaaSアプリケーションに対する手動の監査の適用範囲

SaaSアプリケーションを手動で監査している場合、次の領域でどの程度のカバレッジが得られますか？

悪意のあるサードパーティアプリケーションに遭遇した経験はありますか？

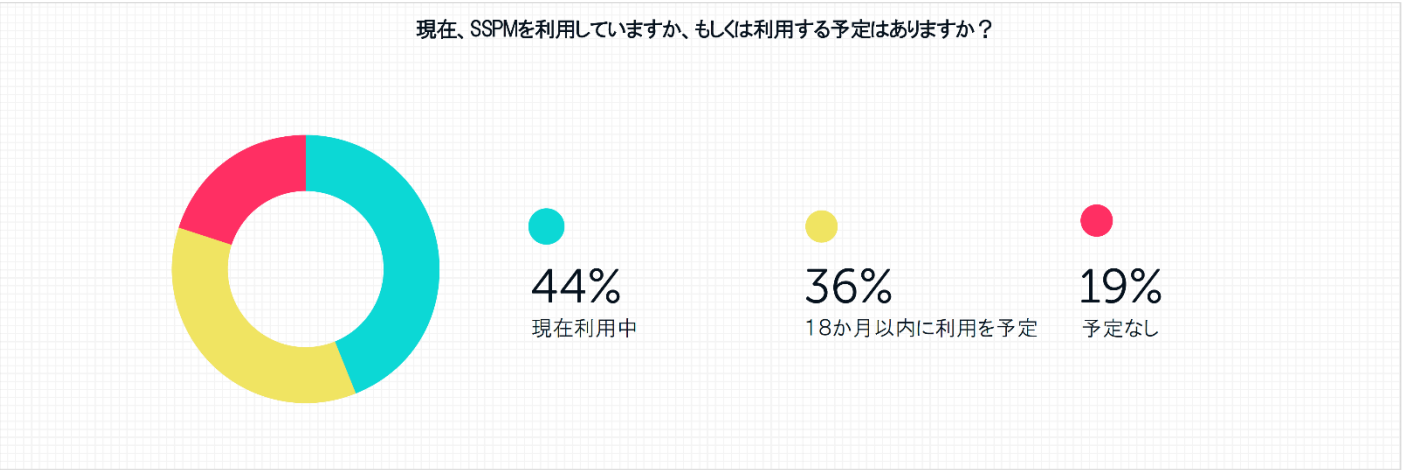


SaaSアプリケーションのセキュリティインシデント



SSPMの利用と効果

SSPMを利用中または利用予定



SSPMを使用することで得られる主なメリット

- 35% SaaSランドスケープに対するコントロールの向上
- 34% SaaSのセキュリティを高める
- 19% 管理・保守の時間短縮 管理・メンテナンスの時間短縮
- 8% コスト削減
- 3% 新しい状況や課題への適応能力

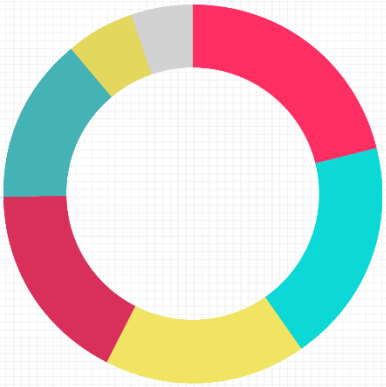
SSPMソリューションに期待される主な効果

- 31% SaaSの脅威を軽減する
- 29% SaaSのセキュリティ態勢を強化する
- 23% 管理・メンテナンスの時間短縮
- 10% コスト削減
- 7% 新しい状況や課題への適応能力

今後18ヶ月以内にSSPMソリューションの導入を予定している回答者の結果。

SSPMを導入しない理由

SSPMを導入する予定がない一番の理由は?



21%
組織の最優先事項ではないため

19%
ソリューション購入の予算不足

17%
導入するための人員と知識の不足

17%
管理するための人員と知識の不足

14%
他のソリューションでカバーしている

6%
この種のソリューションは、セキュリティ上の懸念に合致しない

5%
その他

謝辞

Lead Authors:

Hillary Baron

Contributors

Josh Buker

Marina Bregkou

Ryan Gifford

Sean Heide

Alex Kaluza

John Yeoh

Designer

StudioYael

Special Thanks

Hananel Livneh

Arye Zacks

Caroline Rosenberg

Eliana Vuijsje

協賛企業について

SaaSセキュリティのリーダーであるAdaptive Shieldは、セキュリティチームが脅威の予防、検出、対応を通じてSaaSスタック全体を保護できるようにします。Adaptive Shieldにより、企業はすべてのSaaSおよびサードパーティ製接続アプリを継続的に管理・制御し、すべてのSaaSユーザーとそのデバイスに関連するリスクを管理することができます。Maor BinとJony Shlomoffによって設立されたAdaptive Shieldは、Fortune 500の多くの企業と取引しており、Gartner® Cool Vendor™ 2022に選ばれています。

www.adaptive-shield.com　LinkedInでフォローする　デモを依頼する