sysdig SECURE EVERY SECOND.

2025年版 クラウドネイティブ セキュリティおよび 利用状況レポート

実データ、実在する脅威、真のベンチマーク

目次

主要トレンド

マシンIDはユーザーIDに比べて7.5倍もリスクが高い：管理すべきIDの数は、ユーザーIDの4万倍にもなります。

AI/MLパッケージを使用するワークロードは昨年1年間で500%増加：一方、パブリックエクスポージャーは昨年1年間で38%減少しました。これは、AIのセキュアな実装が企業や組織にとっての明確な優先事項となったことを示しています。

リアルタイム検知と対応を10分以内で実現：ツールが数秒以内にアラートを発行する場合に、これが可能となり、その結果、企業は4分以内に対応措置を開始できるようになります。

コンテナの60%が1分以内の寿命しか持っていません。

実行環境の脆弱性は6%未満に減少：その一方で、イメージの肥大化は前年比で5倍に増加しました。

世界中のあらゆる業種が、その規模にかかわらず、Falcoのような**オープンソースソフトウェアを利用**しています。

サイバーセキュリティ規制は不可欠：EUを拠点とする企業は、グローバル企業に比べてコンプライアンスをより優先することで、サイバーセキュリティ規制を先頭に立って推進しています。

エグゼクティブサマリー

Sysdigの『クラウドネイティブセキュリティおよび利用状況レポート』は今年で8年目を迎えます。同レポートは、実際のデータを利用して、クラウドセキュリティとコンテナ利用の現状を分析するものです。本レポートに記載されている調査結果は、セキュリティチームが主要なすべての分野において大きな進歩を遂げていることを示しています。これは、前年比を見るだけでなく、過去のレポートを振り返った場合にも言えることです。これを念頭に置いて、この2025年度版のレポートでは、成熟度と効率性に関するベンチマークを紹介しています。これらのベンチマークは、セキュリティチーム、開発者、そして組織のリーダーが、来年の進捗を測定するのに役立ちます。

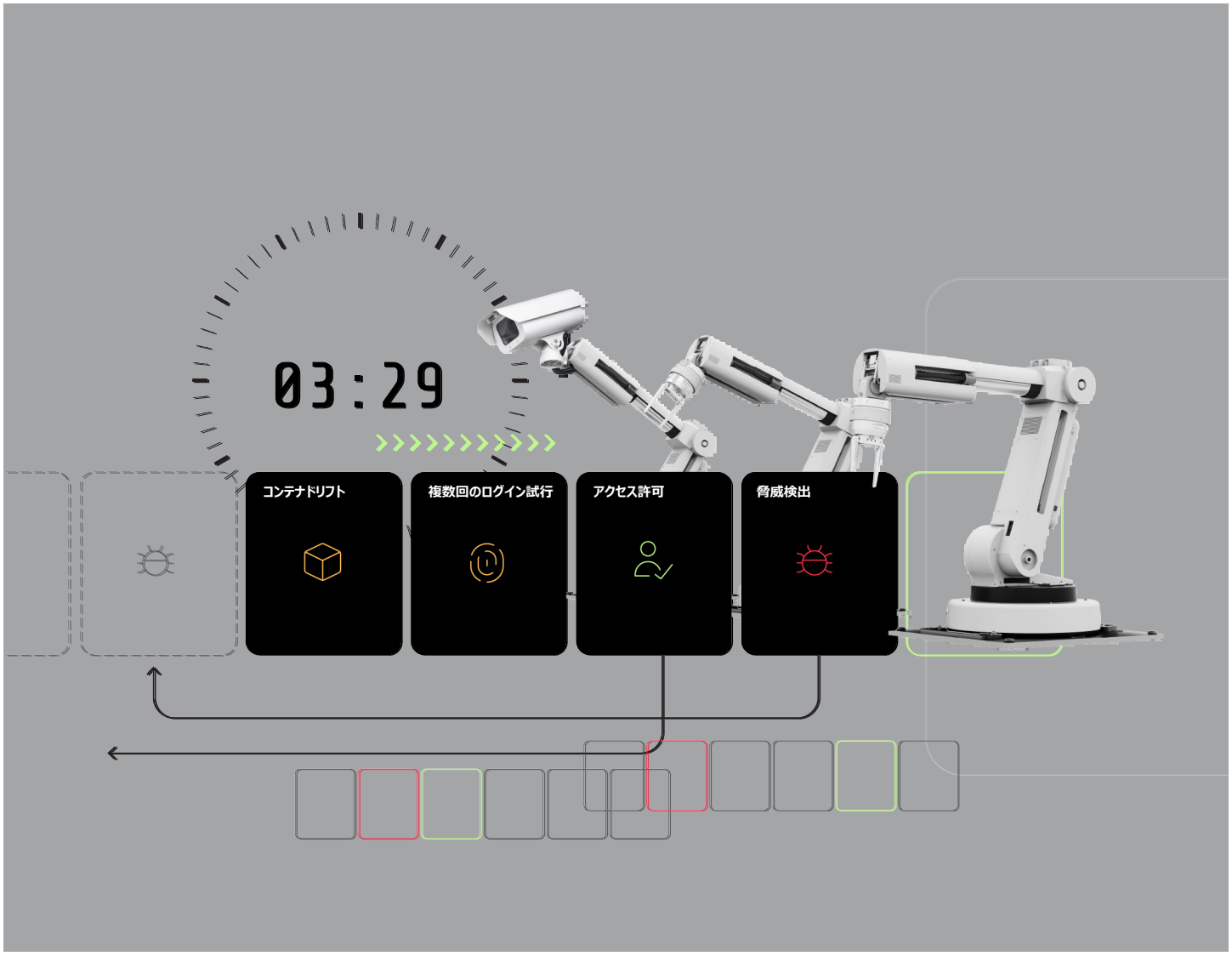
2023年10月、Sysdigの脅威研究チーム（TRT）は、クラウド攻撃は10分以内に行われると結論づけました。本レポートでは、企業や組織が今日、革新的なツールや手法を駆使して、いかにしてこの短いタイムフレーム内において、実際の脅威の検知、調査、対応を行っているかについて詳述しています。また、オープンソースソフトウェアは単なるトレンドではなく、今日のクラウドセキュリティにとって不可欠なものとなっていることも明らかになりました。オープンソースの脅威検知ツールであるFalcoは、1億4千万回以上もダウンロードされており、大企業から中小企業に至るまで幅広く使用されています。これは、あらゆる規模の企業や組織が、オープンソースセキュリティの持つパワーに価値を見出していることを示しています。

セキュリティコミュニティは、脆弱性管理とAIワークロードのセキュリティにおいても進歩を遂げています。2年連続で、ランタイム脆弱性の大幅な減少が確認されました。また、AIや機械学習（ML）パッケージを使用するワークロードの数も大幅に増加しており、このような増加にもかかわらず、ワークロードのパブリックエクスポージャーの割合は大幅に減少しています。これは、企業や組織がAIセキュリティを優先していることを示しています。

過去数年とは異なる視点からID管理を評価した結果、企業や組織はユーザーアカウントよりも飛躍的に多くのサービスアカウントを管理しており、これらのサービスアカウントにはより高いリスクプロファイルが存在していることが判明しました。この事実に基づくと、サプライチェーンへの攻撃がますます一般的になっているのも不思議ではありません。

さらに、意外な事実として、企業や組織がコンプライアンスポリシーのための技術的セキュリティベンチマークをニュースで目にする連邦政府規定の規制よりも優先していることが判明しました。また、当社が長年提供してきたコンテナの寿命に関する統計が新しい形になっていることも付け加えておきます。短命のワークロードは、スピードを実現するために設計されたものであり、タスクを完了するのに十分な時間しか生きられません。リアルタイム検知と継続的な監視が必要なのは、このためです。

以降のページで、今年の全調査結果に関する統計を解説します。



クラウドでの検知と対応を数分で実現

2023年末、Sysdig TRTはクラウド脅威の検知と対応に関するベンチマークを設定し、クラウド攻撃は平均10分で発生すると発表しました。検知に5秒、調査に5分、対応に5分というのは高いハードルのように思えるかもしれませんが、これはセキュリティを確立するために実現可能で、かつ必要なことです。『**2024年度グローバル脅威レポート：年間レビュー**』に記載されているように、今年のクラウドインフラに対する最も一般的な脅威の中には、オープンソースを悪用したものがあり、この傾向は止まる気配がありません。

リアルタイム検知を5秒で実現

残念ながら、アラートはイベントからそのままセキュリティチームに届くわけではありません。信じられないかもしれませんが、データがスキャナーから受信トレイや通知ダッシュボードに届くまでにはいくつかの「ホップ」が必要であり、その時間はすぐにかさみます。データ転送のライフサイクルにおけるエラーは、検知アラートを数分間遅らせる原因となり、タイムリーな対応の機会を事実上なくしてしまいます。

これは実際には何を意味するのでしょうか？本番地域のホストやコンテナからの何10万件ものアラートを分析した結果、ユーザーがイベント通知を受け取るまでにかかる平均時間は5秒未満であり、これはsysdigが提唱している「**クラウドの検知と対応の555ベンチマーク**」と同程度であることが判明しました。攻撃者が数分で組織に大混乱をもたらす可能性がある以上、リアルタイムの脅威検知と対応は不可欠であり、15分以上かかるような遅いやり方は時代遅れになりつつあります。

> 私は、自社の環境で潜在的な脅威が確認されてから15分後にそれを知りたくありません。即座に知る必要があります。脅威が重大な影響を及ぼす前にそれをシャットダウンできるようにするためです。
>
> - BigCommerce社、シニアインフラストラクチャーセキュリティエンジニア、Jordan Bodily氏

インシデント調査を5分未満で実施

従来、企業や組織は、高精度の検知を実現するためにアラート通知を受け取っており、低レベルおよび中レベルのアラートを毎日手動で確認していました。このやり方は、特に設立されたばかりのセキュリティチームや小規模なセキュリティチームにとっては、時間がかかり、高いリスクを伴うものです。

一方、潜在的なインシデントへの初期対応は、経営幹部が干渉するのではなく、セキュリティチームのやりたいようにやらせるべきです。そして、セキュリティチームは自動化された対応策を用意すべきです。さらに、信頼の構築とリスク低減を自らの業務に組み込むべきです。これらは、MITRE ATT&CKフレームワークの広い範囲をカバーする高精度の検知を利用することで達成できます。これは、特定の環境、特定のツール、特定のソフトウェア、そして特定の事業部門に関する脅威を検知するものです。

インシデント調査は、生成AI（GenAI）セキュリティアシスタントの実装における重要なユースケースです。セキュリティアラートを手作業で処理することが望ましい分析方法であったとしても、適切なツールを使用すれば、アラートの発見、理解、相互関連付けをより迅速に行うことが可能となり、かつ重要なインジケーターを見逃すリスクを低減できます。

セキュリティチームがクラウド攻撃に対応できるようにする、迅速かつ堅牢なインシデント調査を行うための最良の選択肢は、怪しい振る舞いをしたIDと、関連するすべてのイベント、ポスチャー、脆弱性の収集と相互関連付けを自動化することです。たとえば、強化された調査とリアルタイムのID相互関連付け機能を使用しているSysdigのお客様は、リソース間の関係と攻撃チェーンへの影響を視覚化して理解することが可能であり、**平均3分半未満で調査を完了し、対応に移行できる**ことが判明しています。この事例も、555ベンチマークにおける「調査に5分」という条件を満たしています。

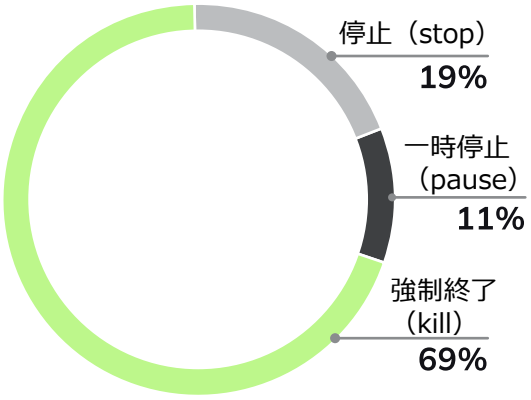
> クラウド環境において、企業や組織は、複数の環境、何千ものID、そして数え切れないほどのワークロードを管理しなければならない場合があります。これらのコンポーネントのランタイムを明確かつ包括的に可視化できなければ、調査に数週間を要することになります。数分で調査する準備ができていなければ、サイバー脅威に打ち勝つことはできません。
>
> - Apree Health社、ITセキュリティ部門シニアマネージャー、Cat Schwan氏

> 以前は、調査に1週間かかることもありましたが、Sysdigを使えば5分から10分の作業で済むようになりました。
>
> - セキュリティオペレーションプロバイダー、情報セキュリティリーダー

インシデント対応を自動化する必要がある

多くのユーザーはまだ慎重であり、コンテナドリフトに関するアラートのみを希望していますが、コンテナドリフトの兆候があった場合に、自動化された予防措置（強制終了、停止、一時停止など）を有効にしていたドリフトコントロールポリシーユーザーの数は、**過去1年間で約3倍に増加**しました。下記の図は、コンテナドリフトに対応するために組織が選択している自動化されたアクションを表しています。

11%以上の顧客が、以下の自動ドリフトアクションのいずれかを選択している。



その一方で、コンテナ内の仮想マシンやサードパーティが所有する自己更新コンテナなどのように、ドリフトと誤認される可能性のあるアクションや振る舞いが複数存在しています。これらの無害なコンテナアクションを自動的に停止または一時停止することは、運用上の不適切な問題を引き起こす可能性があります。このような理由から、ドリフト制御の自動化対応は、企業や組織が保有しているセキュリティプログラムの**成熟度と信頼性**を示す指標の1つであると言えるでしょう。

自社の予防措置を定義する

昨年からコンテナのセキュリティプラクティスが成熟する中で、Sysdigは、脅威の検知やマルウェア関連のインジケーターに対して、信頼性の高い自動対応アクションを実施する次のようなオプションを追加しました。

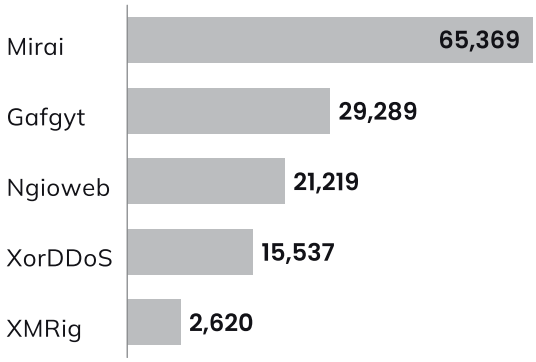
- まず、ドリフトバイナリをコンテナのオリジナルイメージの一部ではなく、通常、実行中のコンテナ内でダウンロードまたはコンパイルされたバイナリとして定義することから始めました。
- その後、ボリュームベースのバイナリを検知する機能を導入し、マウントされたボリュームからすべてのバイナリをドリフトとして扱うようにしました。優れたドリフト検知には、大きな責任が伴います。
- そして、正規表現（RegEx）ステートメントを定義することにより例外を定義できる権限をユーザーに付与しました。このようなきめ細かい例外を定義することにより、特定のファイルやバイナリを、Sysdigエージェントがドリフトとして誤検知することなく実行できるようになります。

誤動作を起こしたコンテナを自律的に強制終了、停止、一時停止させるだけでなく、脅威検知のアラートに従って、ユーザーが自動的にプロセスに「**kill -9**」コマンドを発行することもできます。さらに、フックを介してシステムレベルでドリフトやマルウェアを自律的に防止することも可能です。この追加ステップでは、ポリシーが有効でスコープされている必要があるため、すべての実行試行がエージェントに問い合わせた上で、当該ポリシーが適用可能かどうかに基づいてアクションを確認または拒否することになります。このような確認は、セキュリティポリシーのリアルタイムな実施を保証するため重要であり、これにより、未承認の活動や悪意ある活動を、それらがランタイム環境を侵害する前に防ぐことが可能となります。

最もホットなLinuxマルウェアはオープンソースである

Sysdig TRTは、272,000件を超えるマルウェアのハッシュを分析し、過去1年間に最も一般的に使用されたLinuxマルウェアのファミリーを特定しました。その結果、最も一般的なマルウェアの亜種は「Mirai」であったことが判明しました。Sysdig TRTは、このようなオープンソースのマルウェアコードを使用した攻撃について頻繁に報告しています。これには、DDoS-as-a-Serviceを提供するボットネットグループである**RebirthLtd**などが含まれています。

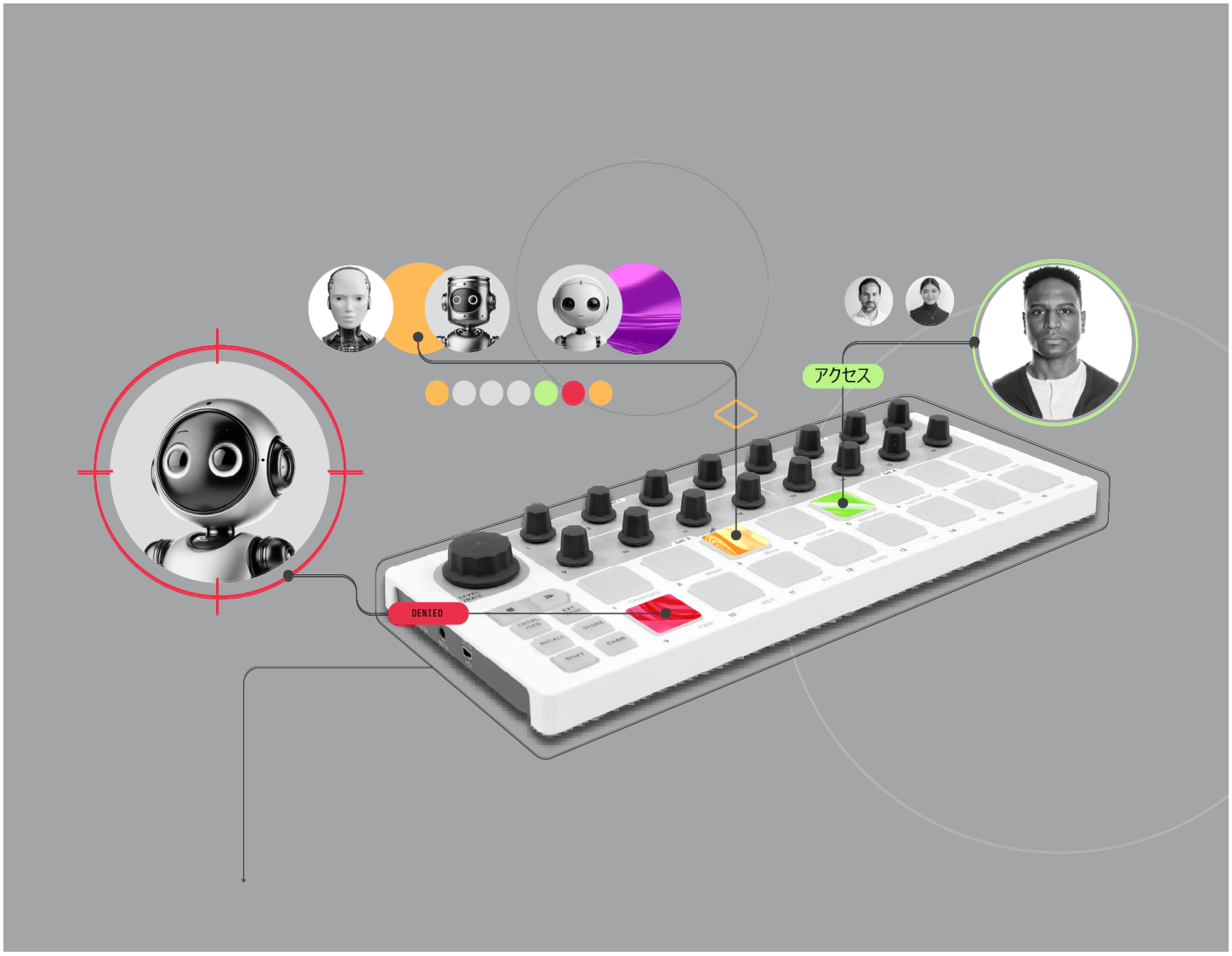
下記の表は、2024年において最も一般的な5つのLinuxマルウェアファミリーのリストです。



セキュリティチームは、脅威インテリジェンスを定期的に使用して、静的な脅威の検知を改善強化すべきです。昨年の調査では、攻撃の35%はIoC（侵害の痕跡）ベースの検知で特定できました。しかし、攻撃者は、これらの検知を回避するためにマルウェアのハッシュを簡単に変更できるため、そのような検知では役に立ちません。脅威の検知と対応には、より広範な脅威の状況を捉えるような階層型のアプローチが不可欠です。攻撃者が成熟し、従来のシグネチャベースの検知を回避するようになるにつれ、振る舞いベースの検知を必要とする攻撃の数は今後も増え続けるでしょう。

2024年における脅威の傾向の1つとして、オープンソースツールを悪意ある目的で活用する攻撃者の急増が挙げられます。

『2024年度グローバル脅威レポート：年間レビュー』を読む →



ユーザー、マシン、そしてそれらの中間にあるあらゆるIDを管理

クラウドセキュリティにおいて、鉄壁のID管理と強固なIDセキュリティが必要であることは周知の事実です。Google Cloudの「**H1 2024 Threat Horizons Report**」によると、2024年上半期のクラウド環境の47%では、脆弱な認証情報や紛失した認証情報が最初のアクセスベクターとなっています。効果的かつ適切に管理されたID管理は、攻撃のリスクを減らす最も基本的な（しかし複雑でもある）方法の1つです。その理由をいくつか探ってみましょう。

クラウドサービスプロバイダー間でIDを比較する

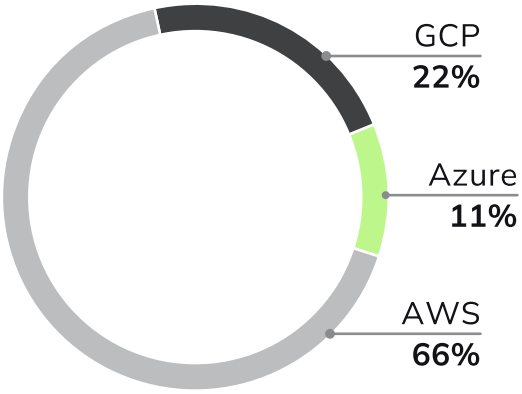
ID利用データを分析したところ、各クラウドサービスプロバイダー（CSP）内で維持するユーザー数に興味深い異常があることが判明しました。この異常は、マルチクラウドユーザー間でも見られました。Azureは、アマゾンウェブ サービス（AWS）やGoogle Cloud Platform（GCP）よりも最大67倍も多くの「ユーザー」を抱えていたのです。興味をそそられた私たちは、さらに調査を進めました。

Entra ID（旧称Azure Active Directory）に依存する新しいアプリケーションにユーザーがログインするたびに、新しいAzureユーザーが集計されていることにすぐに気づきました。これには、Microsoft Officeアプリケーション、サービスメール、メーリングリストなどが含まれます。言い換えれば、これらの「ユーザー」の中には、Azureクラウドポータルにアクセスできる人間もいるかもしれませんが、その大多数はシングルサインオン（SSO）とOfficeに限定してMicrosoftを使用している可能性が非常に高いと思われます。

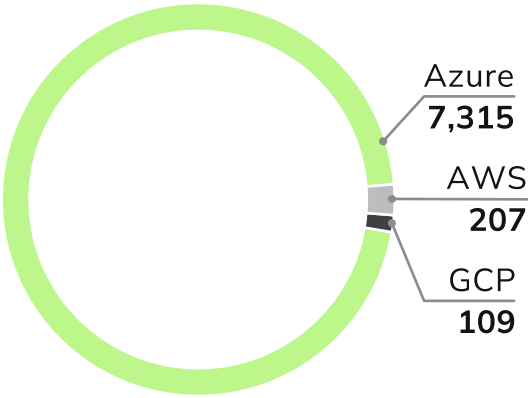
たとえば、Outlook、OneDrive、OneNote、PowerPoint、Excel、Wordにアクセスできる社員は、Azure上に7ユーザー分のアカウントを持ちます。

GoogleとAWSはこのようなディレクトリやIDソリューションを持たないため、Azure CSP組織のユーザー数は非常に偏っていることになります。

CSP別の「IDを保持している組織」の割合



CSP別の平均ユーザー数



過剰な権限の克服

ID管理は多くの場合、時間がかかり維持するのが困難な作業です。**2024年版のレポート**では、過剰なリスクを管理しており、付与された権限の98%が使用されていないことが判明しました。過剰な権限付与は、ほぼすべてのセキュリティ専門家が忠告しているにもかかわらず、仕事を終わらせるための最も迅速で簡単な方法となっているのです。

過剰な権限は理想的とは言えず、脅威アクターに初期アクセス、ラテラルムーブメント、機密データへのアクセスなどの不当な機会を与えることで、クラウド侵害のリスクを大幅に増大させます。しかし、組織によっては、それを「業務運営を迅速化するために許容できるリスク」として考えているところもあります。このような場合、多要素認証（MFA）などのセキュリティ対策を積極的に実施することで、ID攻撃のリスクを低減し、潜在的な攻撃を検知してその影響を軽減できるようになります。

過剰なIDがもたらす不必要なリスクを最小限に抑える

では、過剰な権限が容認されているとしたら、組織はどのくらいの数のIDを管理しているのでしょうか？平均で915のユーザーと41,605のサービスアカウントがあることが判明しました。これは、CSPに接続されるIDの種類によって**40,000倍の差**があることを意味します。

幸いなことに、この統計はプロビジョニングの不備によるノイズによって歪められており、これらの過剰なIDはセキュリティリスクとしては低いと主張することもできます。しかし、160万を超える未割り当てのサービスアカウントを持つ組織は、事故が起こるのを待っている可能性があります。未使用のアカウントは、使用中の脆弱性に比べて優先順位が低くなります。いくつかのデータ操作を適用し、過剰なユーザー（Azureを使用している組織）または過剰なサービスアカウント数を持つ組織の11%をフィルタリングした結果、平均値は「152のユーザーと5,330のサービスアカウント」というより現実的なものとなりました。これは、管理すべきサービスアカウント数がユーザー数の35倍となっているものの、40,000倍よりは納得しやすい数字となっています。

とは言うものの、15%近くの組織では、接続されているユーザーアカウントが存在しないことが判明しました。これは、組織がクラウドアイデンティティアクセスを適切に管理していることを意味しており、セキュリティが成熟していることの確かな証です。このような組織は、クラウド環境やリソースにアクセスするために、従来のローカルユーザーとパスワードの組み合わせを確立して維持するのではなく、サードパーティが提供するSSO認証プロセスを使用してクラウドアカウントにログインしている可能性が高いと思われます。今もなおログインしている人間のユーザーはいますが、サードパーティの検証サービスを使用することでセキュリティレイヤーが追加されているため、それらはユーザーとしてカウントされていないのです。

約15%の組織では、**接続されている**
ユーザーアカウントが存在しません。

ID関連のリスクを定義する

組織が持つリスクに対する認識は、その組織がどのような定義に従うかによって決まります。

本レポートのデータ収集と分析において、「リスクのある」ユーザーを、MFAが有効でないユーザー、またはアクセスキーがローテーションされていないユーザーと定義しました。この定義に従った場合、リスクのあるユーザーを保持している組織はわずか8%でした。

一方、「リスクのある」サービスアカウントとは「アクセスキーをローテーションすることなく管理者レベルのアクセス権を持っているAWSサービスID、Azureプリンシパル、GCPアカウント」と定義しました。この定義に従うならば、実に60%の企業がリスクのあるサービスアカウントを保持しており、この割合はリスクのあるユーザーを保持している企業の7.5倍になります。

これは、ユーザーアカウントをより適切に構成しており、おそらくはユーザーID管理を優先していることを意味します。

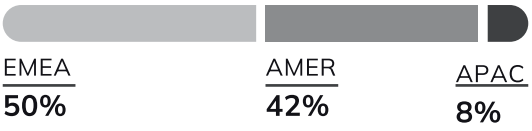
しかし、残り92%のリスクのないユーザーにも、まだリスクの懸念があります。攻撃者は、リスクのあるユーザーであれリスクのないユーザーであれ、標的型スピアフィッシングを通じてアクセス権を取得できるからです。このような脅威を周知させるためには、組織内の全従業員を訓練することが不可欠です。

攻撃者がAIを利用してスピアフィッシングキャンペーンの標的設定、成功率、規模を向上させている中で、このことは特に当てはまります。サイバーセキュリティを確立することは、組織全体の責任です。このようなリスクのあるユーザーは、管理者やテストアカウント用の、許容可能な既知のリスクプロファイルである可能性が高いと思われます。

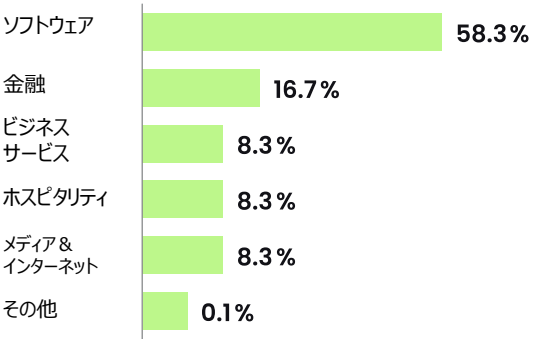
リスクのあるサービスアカウントについては、単純な対策から始めます。レガシーベンダーは、現在でも寿命の長い鍵の使用を許可しており、組織がこれらを使用している場合、それらを安全に保管し、ローテーションする必要があります。また、組織は、正確に定義された信頼関係を使用して、人間のユーザーやサービスアカウントが他のIDになりすまして、他のリソースに一時的にアクセスできるようにすることも可能です。信頼関係もまた、セキュリティを強化し、管理を簡素化します。なぜなら、認証情報や過剰な権限が不要なため、攻撃者が最初にアクセスする機会を減らすことができるからです。

リスクのあるユーザー

地域

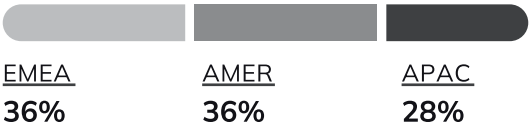


業種

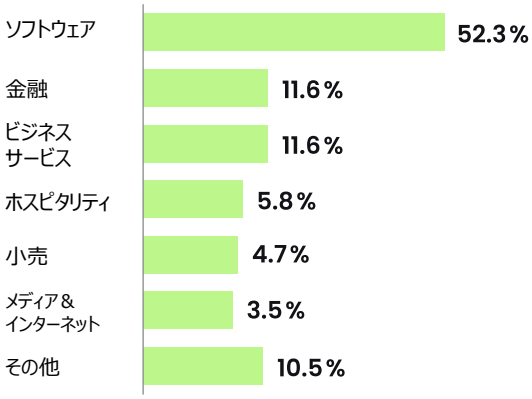


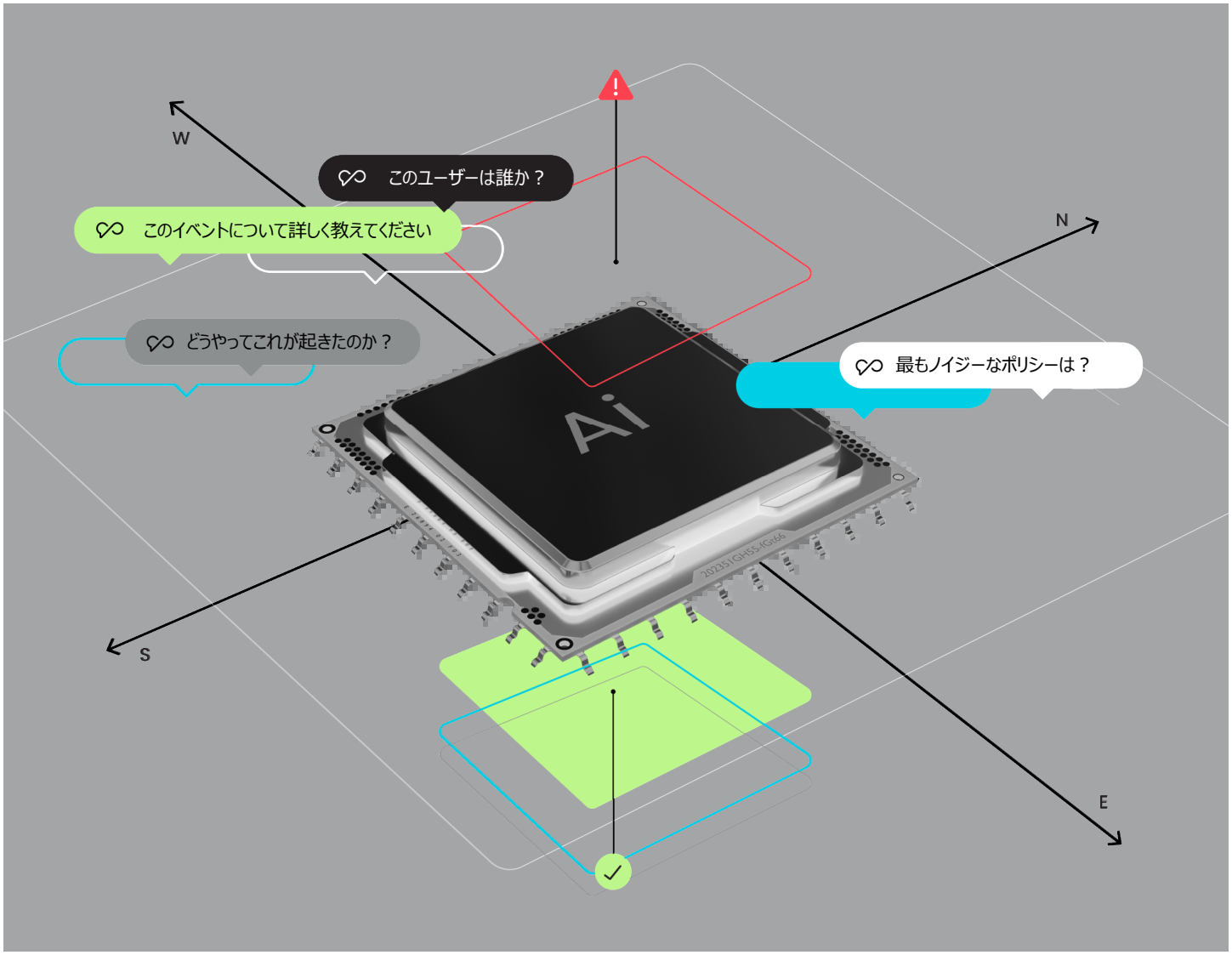
リスクのあるサービスアカウント

地域



業種





セキュアなAIを通じて リスクとリターンを ナビゲートする

2022年11月にChatGPTが一般公開されたことで、2年以上にわたってAIの普及を経験してきました。AIのセキュリティに関する懸念は一般的に、AIを利用してセキュリティ対策を強化する方法と、AIそのものを保護する方法の2つに分類されますが、どちらも妥当なものです。しかし、利用が拡大する一方で、楽観視すべきAIセキュリティのトレンドも数多く見られるようになりました。

セキュリティ用のAIの導入は増加傾向にある

2024年4月に発表されたCloud Security Allianceの「**State of AI and Security Survey Report**」によると、2024年に生成AIソリューションの導入を計画している企業は55%に上りました。企業は生成AIの導入に熱心だったのです。業界初の生成AIクラウドセキュリティアナリストである**Sysdig Sage™**が一般提供されてから4ヶ月以内に、Sysdigの顧客の45%がこれを有効にしました。

生成AIは多くのプロフェッショナルの日常業務に組み込まれており、サイバーセキュリティも同様です。Sysdig Sageユーザーの75%は、自らをセキュリティオペレーション（SecOps）チームの一員であると認めています。Sysdig Sageは、彼らがアラートをトリアージし、脅威を特定し、異常なパターンを発見するのを効果的に支援しています。

> 攻撃者はすでに日常的にAIを利用しているため、セキュリティチームは後れを取るわけにはいきません。私は、現在AIをある程度活用していないセキュリティプラットフォームを信用しませんが、誇大広告を盲目的に信じているわけでもありません。すべてのAIが同じように作られているわけではなく、見せかけのチャットボットには反応しないことが重要です。真に価値があるのは、実際に効率を高め、人間の対応を迅速化し、戦力として機能するようなAIなのです。
>
> - Sprout Social社、シニアセキュリティエンジニア、Brayden Santo氏

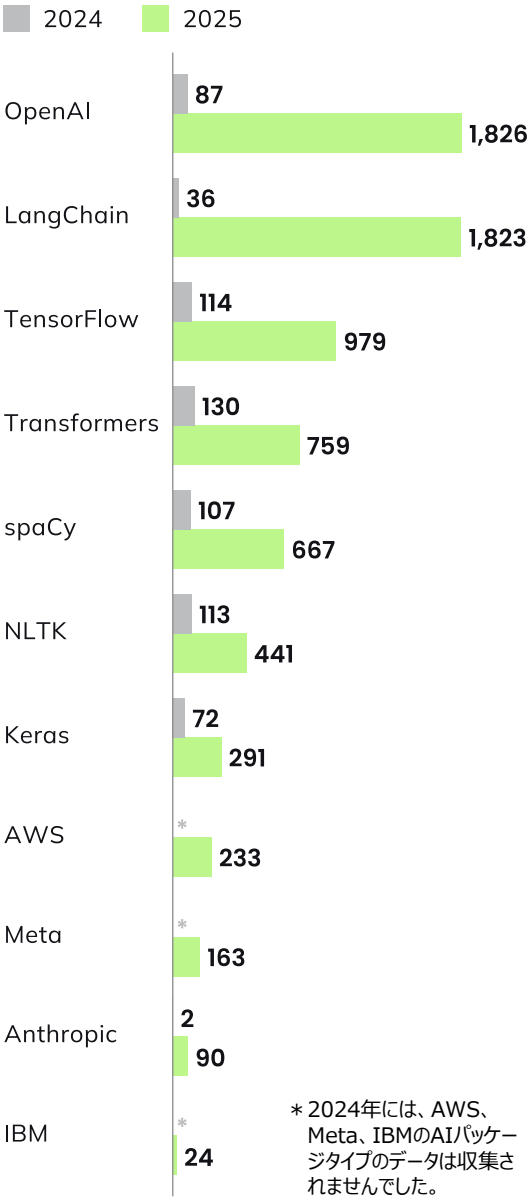
AIを利用したセキュアなワークロード

企業環境におけるAIツール、特に大規模言語モデル（LLM）の使用は、データガバナンス、データセキュリティ、およびデータ主権に関する懸念を引き起こします。ユーザーが最もセンシティブな専有データや顧客情報の一部をAIモデルに投入する可能性があるため、多くの企業はSysdigの**AIワークロードセキュリティ**のようなツールによる脆弱性管理を優先し始めています。

当社の顧客の75%がAIまたはMLパッケージを使用しており、これは昨年のレポートから2倍以上に増加しています。さらに、**ワークロード内で実行されているAI/MLパッケージの数も、昨年から500%近く増加しています。**

2024年のレポートでは、顧客のAI/MLパッケージのうち、特に生成AIに特化したものは15%に過ぎず、残りはデータの相互関連付けや分析に通常使用されるツールでした。生成AIパッケージの割合は、15%から36%へと、昨年1年間で2倍以上に増加しています。パッケージの種類の内訳に関しては、右図をご覧ください。

AIパッケージの種類



＊2024年には、AWS、Meta、IBMのAIパッケージタイプのデータは収集されませんでした。

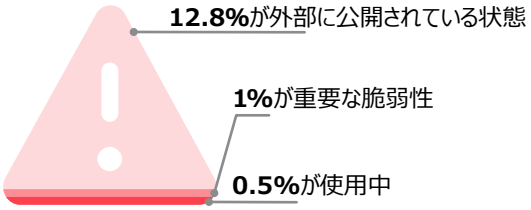
生成AIパッケージの割合は15%から36%へと、**この1年で2倍以上に増加**しました。

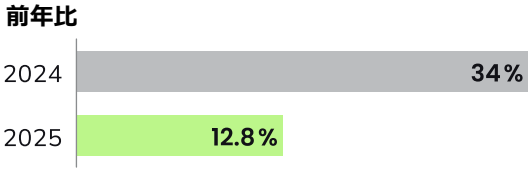
しかし、これらのパッケージはどの程度セキュアなのでしょうか？2024年4月、AIパッケージを含む顧客のワークロードの34%がパブリックエクスポージャー状態になっていました。パブリックエクスポージャーとは、適切なセキュリティ対策を講じることなく、インターネットや他の信頼できないネットワークからワークロードにアクセスできる状態を指しており、これはAIモデルによって活用される可能性のある機密データを不必要に危険にさらすことになります。AIの導入が急速に進む中でも、このパブリックエクスポージャー率は13%未満に減少しており、8カ月間で38%減少したことになります。

このようなリスクの低減は、おそらくAIツールの新機能に起因するものであり、AIとサイバーセキュリティについて言及されるたびに浮上するセキュリティ上の懸念に関する当然の精査と一致しています。企業環境にAIをいち早く導入した企業の多くは、技術革新とセキュリティの優先順位付けの両面で最先端を走っているため、このようにAIのセキュリティポスチャーが急速に向上していることは驚くべきことではありません。

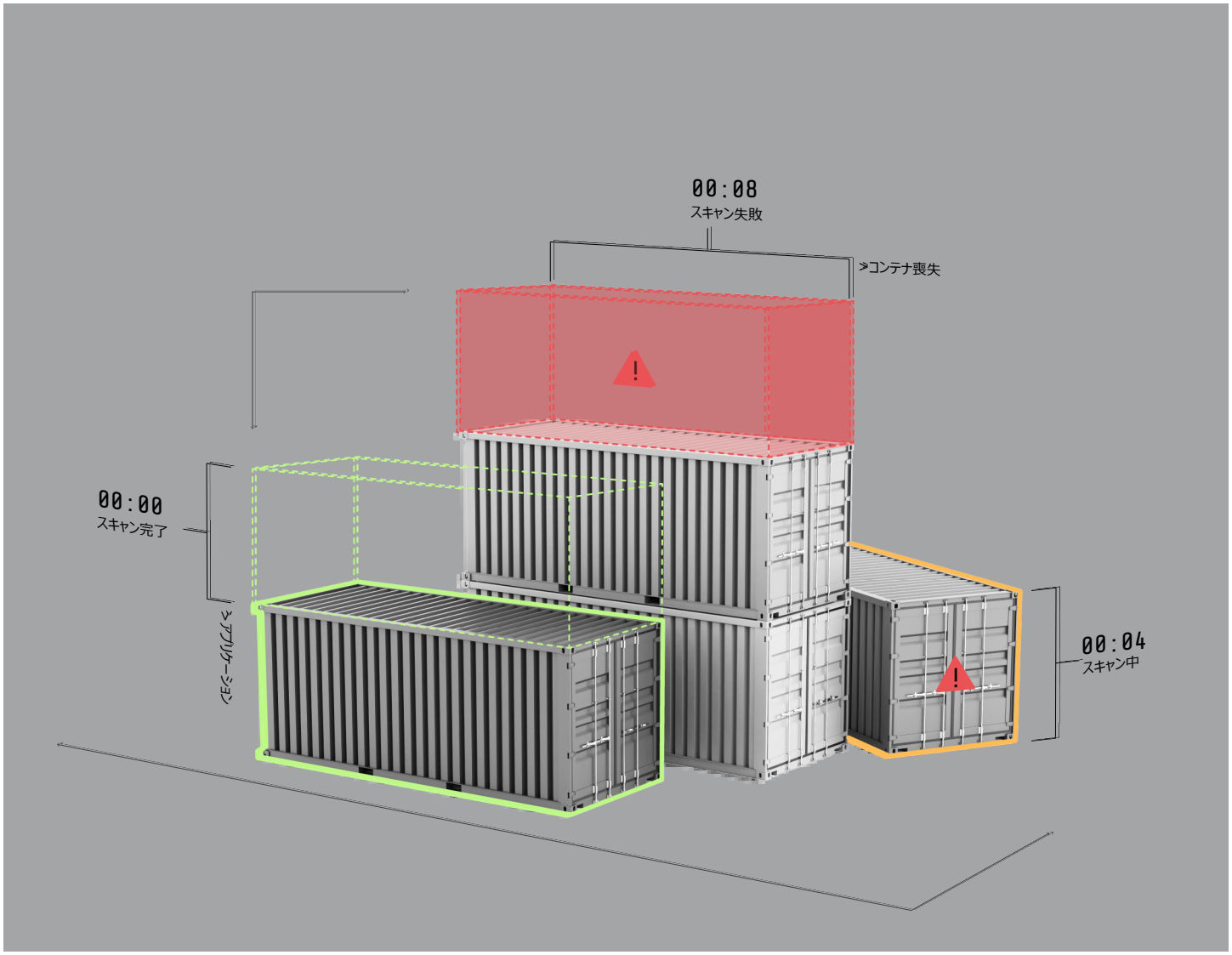
AIを含むワークロードの外部公開状況

2025年、AIパッケージを含むワークロードの**12.8%**が外部に公開されている状態になっている





外部公開率は13%未満に減少し、**8カ月間で38%減少した。**



コンテナ化された環境における リスク管理

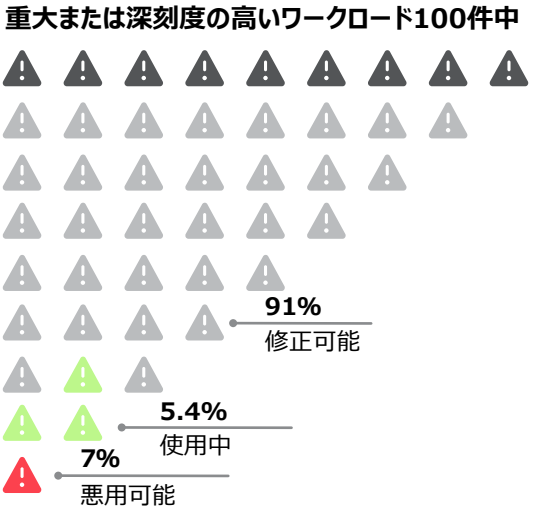
脆弱性管理を優先

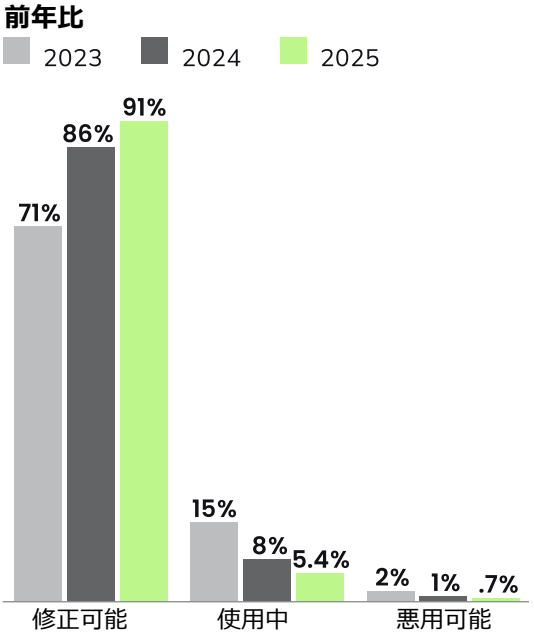
Sysdigを含むセキュリティプロバイダーは、ここ数年間一貫して脆弱性管理の重要性を主張してきました。当社は2年前に脆弱性の状況を分析し、最も効果的で最適な優先順位付けの方法を提示しました。当社では、使用中の脆弱性を「実行中の環境でアクティブにロードされ使用されているパッケージに関連する脆弱性」と定義しています。このデータを毎年見直しており、重要でない何千もの脆弱性に対処する前に、最も重要な脆弱性に適切に優先順位を付けることで、運用上のリスクを劇的に削減し続けていることを発見しました。

当社は、実行環境における脆弱性の優先順位付けと修復の追跡を開始して以来、組織の脆弱性管理における目覚ましい改善を目の当たりにしてきました。毎年、前年よりも多くのワークロードを分析していますが、以下に示すように、使用中の脆弱性に焦点を絞ったことが功を奏しています。分析したイメージのうち、重大または深刻度の高い脆弱性があったのは17%未満でした。

修正プログラムが提供されていて使用中ではない重大で高リスクの脆弱性の割合は、年々増加しています。しかし、これは問題ではありません。というのも、これらの脆弱性は本番環境には存在しないと想定できるため、優先順位付けにおいて本番環境に存在している脆弱性よりも優先順位付けが後回しになるからです

重大で深刻度の高い脆弱性





イメージの肥大化を抑える

イメージの肥大化、つまりアプリケーションを適切に実行するために必要でない余分なパッケージを含めることは、さらなるリスクと不必要なコストをもたらします。理想的には、イメージは自らのジョブをうまく遂行するのに必要となるコードだけを含むべきです。残念ながら、イメージの肥大化の問題は増加傾向にあるようです。

イメージの肥大化は昨年1年間で5倍になり、肥大化したイメージはまだコンテナイメージ全体のごく一部に過ぎないものの、コンテナイメージに含まれるパッケージの数も全体で300%増加しています。繰り返しますが、これはコストとセキュリティリスクの増大を意味します。

パッケージやイメージの肥大化にはいくつかの理由が考えられますが、これらの増加は、開発者が開発を迅速化するために、容易に利用可能なライブラリや肥大化したオープンソースソフトウェアを単純に追加したことによるものと考えられます。その理由の1つは、「AIを使用するセキュリティワークロード」で述べたように、AIを含むオープンソースやベンダーが管理するワークロードが急速に増加し、500%も増加していることに起因している可能性があります。端的に言えば、多くの企業が、新しいアプリケーションや変更されたアプリケーションをより早く出荷するために、あらゆることを試しているのです。

イメージの肥大化を抑えるには時間がかかりますが、ベースイメージを定期的に監査することで軽減できます。AIツールを使って未使用のパッケージをスキャンし、特定することも検討しましょう。必要であれば、調査結果のレビューを手動で行うこともできます。

イメージサイズが小さくなれば、脆弱性は少なくなり、アタックサーフェスも縮小できます。アプリケーションデリバリー、CI/CDパイプライン、脆弱性スキャナーは、イメージが小さいほどより速く実行され、より多くのコストを削減できます。より小さなワークロードを実行することで、より少ないストレージ、より広いネットワーク帯域幅、より少ないコンピューティングリソースを使用することになります。これぞまさにWin-Winです。

イメージの肥大化は昨年の**5倍に増加**しました。

コンテナの寿命を最適化する

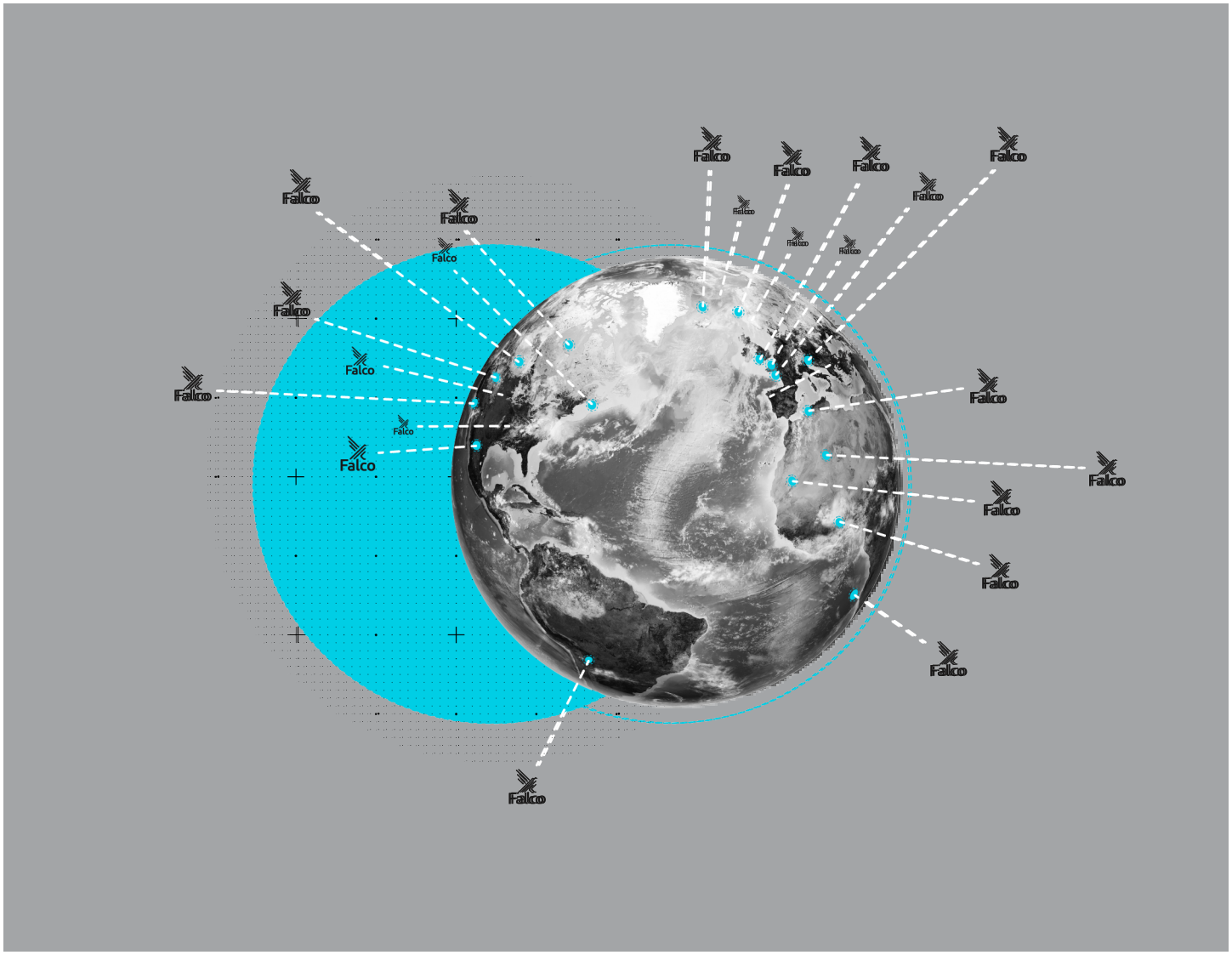
Sysdigは2018年以来、年次レポートでコンテナの短命性について報告してきましたが、2023年以降、70%を超えるコンテナの寿命は5分以下となっています。今年のデータによると、コンテナの74%の寿命は5分以下となっています。また、**コンテナの60%の寿命は1分以下**であり、そのうちエラーが原因となっているのはごく一部であることも判明しました。

コンテナの寿命が1分未満になる理由をいくつか見てみましょう。

- **専用に設計された短命タスク：**コンテナは、仮想マシンよりも高速かつコスト効率よくアプリケーション全体を格納して実行できます。最新のアプリケーション開発では、コンテナはより区分化された方法で使用されます。コンテナは、非常に短時間で実行されるスクリプトまたはプロセスの一部のみを実行するなど、短時間のタスクに使用されます。これには、バッチ処理、テスト実行、データ変換、CIパイプラインの実行などがあります。タスクが完了すると、コンテナは存在しなくなります。
- **サーバーレスまたはマイクロサービス設計：**サーバーレスおよびマイクロサービスのクラウドアーキテクチャでは、機能やサービスは、目的に応じて構築された短命のタスクと同様に、単一のリクエストまたはジョブを処理するために短時間実行されるように設計されています。たとえば、コンテナは単一のAPIリクエストを処理するためにスピンアップされ、処理が完了した時点で終了します。
- **リソースの制約：**場合によっては、コンテナはリソースの制約やオーケストレーターポリシーによって意図的に制限されます。たとえば、Kubernetesポッドの準備状況または生存状況のプローブが失敗すると、ポリシーチェックによってアラートが開始され、人間がエラーを確認してコンテナを再起動するまで、リソースを節約するためにコンテナが一時停止またはシャットダウンされることがあります。
- **ヘルスチェック：**Kubernetesワークロードは積極的なヘルスチェック設定を持つ場合があり、指定された短いタイムフレーム内にレディネスチェックに合格しない場合、当該コンテナは終了させられます。
- **クラッシュまたは設定ミス：**アプリケーションコードまたは設定に問題がある場合、コンテナは起動後すぐに失敗する可能性があります。一般的な原因としては、環境変数の欠落、依存関係の誤り、ランタイムエラーなどが挙げられます。

コンテナベースの環境では物事が急速に変化するため、リアルタイムセキュリティは単に「あれば良い」というものではなく、必須となります。コンテナが停止する前に、手動でJiraチケットを送信してインシデント対応を開始するには時間が足りません。

2つのセキュリティプロセスを実装することで、短命なコンテナに対抗できます。まず、アドミッションコントローラーを使用して、クラスター内で実行できるものを定義しカスタマイズします。このプロアクティブな対策により、イメージが安全でない場合、ポッドの実行がブロックされます。次に、コンテナドリフト制御などの高精度の自動応答アクションを実装することで、アクティブな本番環境で悪意ある振る舞いの可能性がある場合に、コンテナをリアルタイムで一時停止または停止できるようにします。これにより、悪意あるアクセスがさらに軽減され、インシデント対応のための余裕が生まれます。



Falcoとオープンソース セキュリティの採用

Falcoは、コンテナ、ホスト、Kubernetes 環境などにおける異常なアクティビティを検知するオープンソースツールです。Falcoは、クラウドネイティブコミュニティ全体で広く採用されており、カスタマイズ可能なルールを使用して、リアルタイムの脅威検知とシステムコールおよびアプリケーションの振る舞いの継続的な監視を行います。

Falcoは2024年2月に重要なマイルストーンを達成しました。それは、Cloud Native Computing Foundation（CNCF）内におけるグラデュエーション（卒業）ステータスを達成したことです。これは、Falcoの成熟度、広範な使用、ガバナンス、および本番環境での実績を反映しています。FalcoはもともとSysdigによって開発されたものであり、2018年にCNCFに寄贈されました。Falcoの持つ勢いは誰も否定できません。Falcoのダウンロード件数が1億に到達するまでに8年かかりましたが、この数字はFalcoがCNCFにおけるグラデュエーションを達成してから50%近く急増しています。現在、このプロジェクトは世界中のユーザーによって1億4千万回以上ダウンロードされています。

Falcoエコシステムの開発と成熟

Falcoはコミュニティ主導の脅威検知プロジェクトであるため、その使用と進化はセキュリティチームと開発チームのニーズを反映しています。Falcoは侵入検知システム（IDS）として始まり、その後、完全に機能するオープンソースのクラウド検知および対応（CDR）ツールへと進化しました。

Falcoは、システムコールを監視するカーネルモジュールと共に、2016年5月にGitHubに初めて登場しました。2年後、最初のeBPF（Extended Berkeley Packet Filter）プローブが導入され、さらに最近では最新のCO-RE（compile once-run everywhere）eBPFプローブが導入されました。eBPFは現在、システムコールを収集するための推奨方法となっていますが、多くのホストは依然としてeBPFをサポートするには古すぎるカーネルを実行しています。Falcoは、カーネルモジュール、eBPFプローブ、およびCO-RE eBPFプローブの3つのドライバーを提供することで、これらすべてのシナリオに対応しています。これにより、あらゆるホスト上で包括的な脅威検知が行えることを確実にしています。 .

303

out of 500

フォーチュン500社のうち
300社がFalcoをダウンロード

Falco

Falcoの歴史

- 2016 — First commit
- 2017
- 2018 — eBPF
  - CNCF sandbox
- 2019 — Falcosidekick
- 2020 — CNCF incubation
- 2021 — Plugins
  - Sysdig donates eBPF libraries
- 2022 — falcoctl
- 2023 — eBPF CO-RE
- 2024 — Talon
  - CNCF graduation

オープンソースはすべての人のためにある

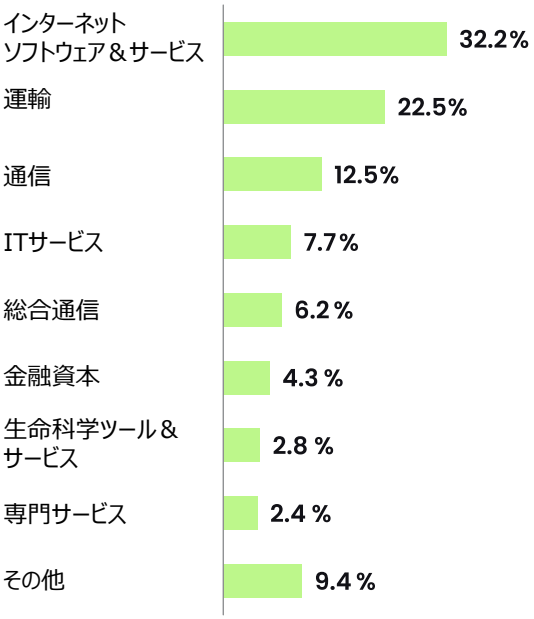
右のグラフにあるビジネスセクターの内訳は、セルフホスト型データセンター内でFalcoを使用している組織のみを対象としています。たとえば、パブリックCSPを使用している企業は、自社のIPアドレスではなくCSPのIPアドレスに関連付けられているため、セクターの区別は不可能です。この理由により、Falcoユーザー間のビジネスセクターの分類は制限されています。

それ以外の場合、ユーザーの大多数がインターネットソフトウェアおよびサービス企業に分類されることは驚くことではありません。これらの組織は、オープンソースソフトウェアコミュニティの利用、同コミュニティとのコラボレーション、および同コミュニティへの貢献をサポートする傾向があり、これはペースの速いビジネスセクターにおけるイノベーションの促進に役立ちます。

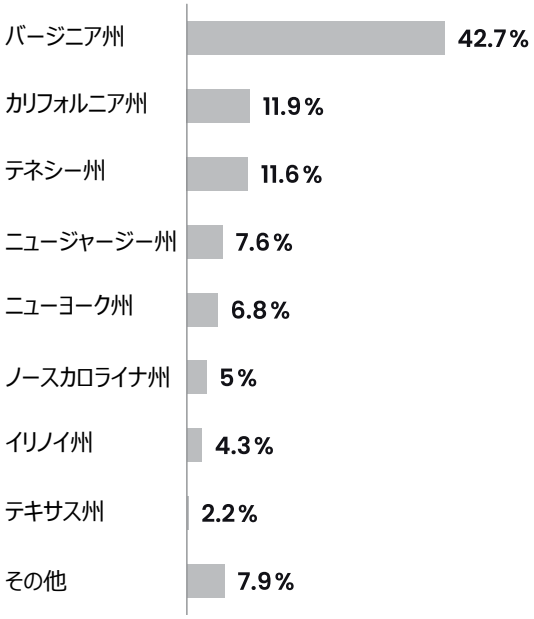
しかし、さらに驚くべきことは、ユーザーの22%以上が運輸業界で働いていることです。運輸業界でFalcoがこれほど多く使用されているのは、組織全体に広く導入されている非常に大規模な企業によるものと考えられます。その結果、運輸業界でFalcoを使用している企業は、インターネットソフトウェアおよびサービス企業よりも少なくなっていますが、運輸業界内でこのツールを使用している個人の数は多くなっています。

米国では、連邦政府のさまざまな組織と契約している企業が集中して存在しています。これらは、中小企業、新興企業、大企業として認められています。これらの契約企業は、首都ワシントンD.C.の近くに大きな拠点を構えており、バージニア州のユーザー数が多いのは、このためと考えられます。この地域に存在する小規模で初期段階の企業にとって、オープンソースの脅威検知ツールの手頃さは見逃せません。テネシー州のユーザー数が多いのは、オークリッジの確立された産業拠点と、ナッシュビルのビジネスおよびテクノロジー企業の大規模な移動と成長によるものと考えられます。

業種別のFalcoユーザー数



米国州別のFalcoユーザー数



Falcoユーザーの世界的な内訳は、世界中でオープンソースとセキュリティの革新に対する情熱と意欲を示しています。それでも、フィンランド(小さな国であるにもかかわらず)のユーザー数が多いのには驚きです。運輸部門でのFalcoの利用状況で見たように、これはおそらく、国内に本社を置く限られた数の組織内で広範な個人による利用が反映された結果だと思われます。これは予想外の事実ですが、間違いではありません。

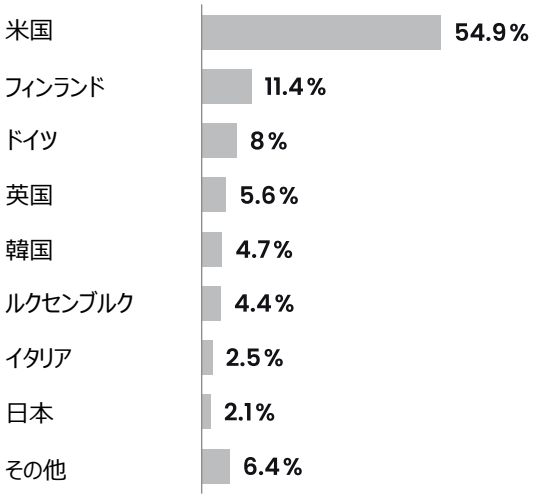
Falcoユーザーの企業規模は、小規模組織と大規模企業がバランスよく混在しています。予想通り、従業員数250人未満の企業のユーザーが34%近くと多くなっています。これらの企業は、有料の脅威検知および対応サービスに資金を投じることができない新興企業や中小企業であると考えられます。

オープンソースの脅威検知ツールには無限の可能性がある

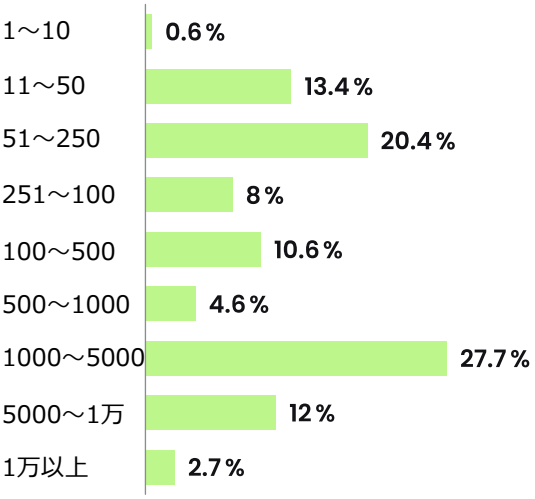
多くの人が大切にしているオープンソースソフトウェアの多くの側面の1つとして、コミュニティ自身が挙げられます。コミュニティはオープンソースツールの改善に直接貢献するだけでなく、ツールの運用エコシステムの成長にも貢献します。Falcoに関しては、検討すべきコンパニオンツールが数多く存在しています。

Falcosidekickは、アラートおよび通知機能を拡張するFalcoの補助ツールであり、ユーザーがFalcoからさまざまなサードパーティのサービスやツールにアラートを転送するのに役立ちます。Falcosidekickの最初のGitHubリリースは2018年10月でした。それ以来、全ダウンロード件数は2,800万回を超えており、2024年だけでも900万回を超えています。そのほとんどは、2024年7月1日の待望のバージョンリリースに続くものです。

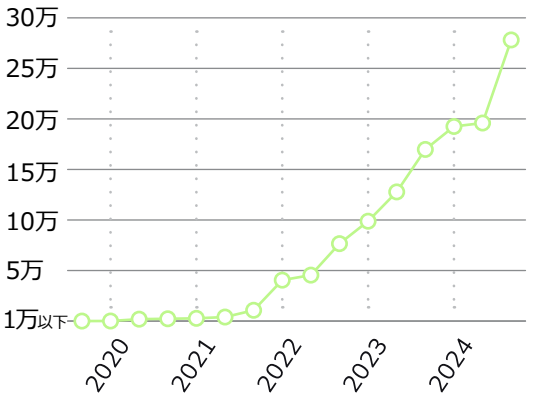
国別のFalcoユーザー数



企業規模別のFalcoユーザー数



日付別のFalcosidekick ダウンロード数



Falco Talonは、ユーザーがFalcoアラートに続いて即座に対応アクションを実行できるようにするコマンド&コントロールフレームワークです。2023年7月に最初に作成され、一般公開バージョンは2024年9月にリリースされたばかりで、2024年末までに約14万回ダウンロードされました。

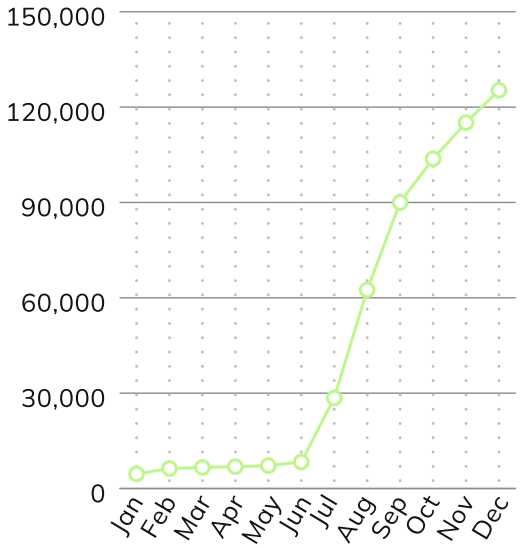
Falcoは、プラグインを介して多くの一般的なセキュリティおよびビジネスツールと統合することもできます。アプリケーションの範囲外でのFalcoの採用と関心は、コミュニティによって作成されるプラグインの数と種類、および新しいプラグインが追加される速度に顕著に表れています。

この傾向は、企業や組織がランタイムを保護するだけでなく、Kubernetes制御プレーン(マネージドかどうかに関係なく)、クラウドアカウント、CI環境などの異常を検知するためにFalcoを使用していることを示しています。**Falcoコミュニティは、今日のサイバー防御業界に必要な「ワンチーム、ワンファイト（one team, one fight）」の精神を体現しています。**

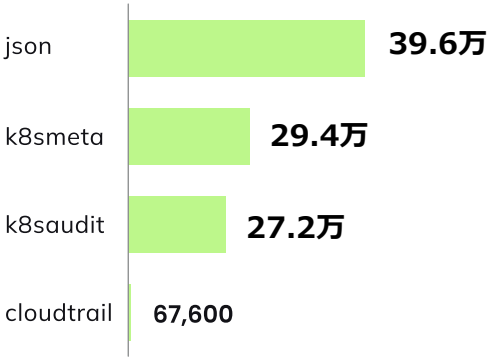
最も人気のあるFalcoプラグインとしては、JSONペイロードからフィールドを抽出する**json**、Kubernetesメタデータを使用してFalcoシステムコールフローを強化する**k8smeta**、Kubernetes監査イベントを読み取り、Kubernetesクラスターを監視するk8saudit、ファイルやS3バケットから**Cloudtrail** JSONログを読み取り、イベントとしてFalcoへとインジェクトするcloudtrailなどが挙げられます。

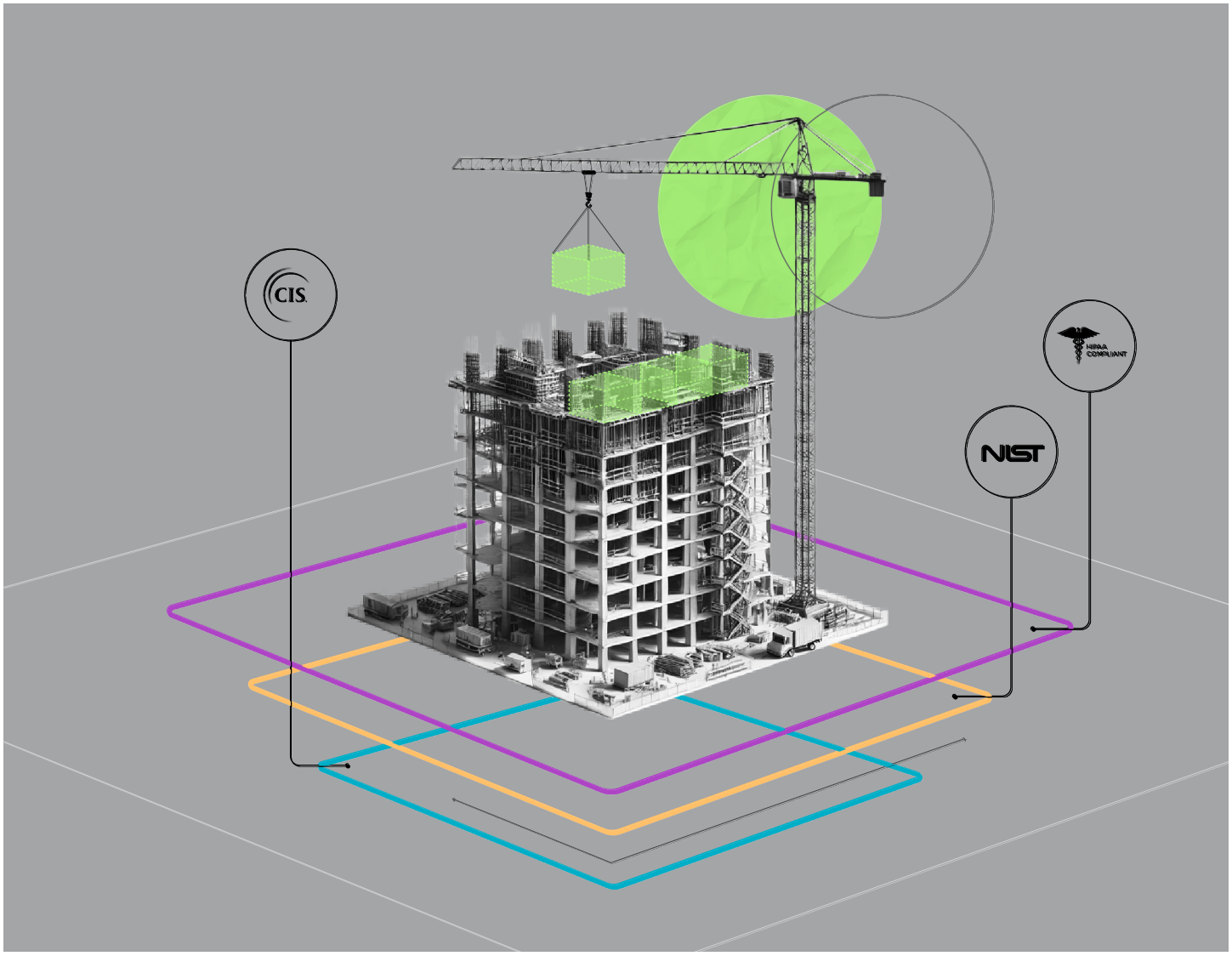
Falcoユーザーによって作成された最も創造的でユニークなプラグインとしては、**Salesforce**用のランタイム脅威検知および監査ログ、**Keycloak**用のユーザーおよび管理者IDアクセス管理イベントログ、**Box**用の脅威検知および監査ログなどが挙げられます。

2024年のFalco Talonのダウンロード数



ダウンロード数別の最も人気のあるプラグイン





»

セキュリティは基礎的なコンプライアンスから始まる

すべての組織は、セキュリティとコンプライアンスの強固な基盤を望んでいます。医療保険の携行性と責任に関する法律(HIPAA)やデジタル運用耐性法(DORA)などのよく知られた規制にはセキュリティ要件がありますが、それらのセキュリティ制御の特異性は、企業がクラウドサービスとITインフラに求める保証を提供するには不十分です。エンジンを組み立てる場合、すべてのコンポーネントがその機能に不可欠であるように、クラウド環境の個々の部分はすべて、必要に応じて機能するように適切かつ安全に構成する必要があります。クラウド環境を管理する場合、基盤に強力なポリシーベースの構成があると、規制への準拠がより容易になります。

コンプライアンスポスチャーを評価したところ、80件を超えるコンプライアンスポリシーのうち、多くの組織が基礎的なセキュリティベンチマークへの準拠を優先していることが判明しました。これらのベンチマークは、Kubernetesのネットワークレベルおよびサーバーレベルにおいて最も詳細なコンプライアンスポリシーを提供します。このようなレベルでのコンプライアンスが成功すると、実践者はセキュアな基盤の上に、より広範で戦略的なコンプライアンスポリシーを構築した上で、他のガイドラインとなる規制に準拠できるようになります。ユーザーが効果的に示したように、これらのポリシーを実装することで、より広範なセキュリティ規制、標準、フレームワークへの準拠を促進する強固なセキュリティ基盤を提供できるようになります。

Center for Internet Security（CIS）ベンチマークと米国国防情報システム局（DISA）のSecure Technical Implementation Guides（STIG）は、特定のオペレーティングシステム、アプリケーション、デバイス、マイクロサービスにおけるセキュリティのベストプラクティスの規範的な評価を提供します。下記の表に示すように、組織によって優先順位が付けられたCISベンチマークとDISA STIGの平均コンプライアンススコアは93%でした。ただし、ベンチマークの一部の側面が組織の環境に適用できないことを考慮すると、下記に示すスコアは偏っており、実際よりも低い可能性があります。

CISディストリビューションに依存しない Linux ベンチマーク（レベル 1 – ワークステーション	100.00%
CIS Kubernetes V1.15 ベンチマーク	100.00%
DISA Kubernetes STIG カテゴリII（中)	98.72%
DISA Kubernetes STIG カテゴリI（高)	97.16%
DISA Kubernetes STIG	96.33%
CISディストリビューションに依存しない Linux ベンチマーク（レベル 2 – ワークステーション)	94.37%
CIS Kubernetes V1.23 ベンチマーク	90.14%
DISA Docker Enterprise 2.x Linux/Unix STIG	88.34%
CIS Kubernetes V1.26 ベンチマーク	81.81%
CIS Kubernetes V1.24 ベンチマーク	81.35%

CISとDISAはそれぞれ、Kubernetesクラスターのセキュリティ保護に特化したセキュリティベンチマークを備えており、コンテナオーケストレーションにおける固有の課題に明確に対処しています。これらは、Kubernetes環境を管理および保守する実務者にとって理想的なものであり、日常的なセキュリティを実現するのに役立ちます。

CIS Kubernetesベンチマークは、コンテナ化された環境に固有のリスクを軽減するために設計された、技術レベルで最もきめ細かなセキュリティベンチマークを提供します。CISは、クラウドプロバイダー、サーバーソフトウェア、オペレーティングシステム、デスクトップソフトウェアなどに対する特定のセキュリティベンチマークを提供します。DISA Kubernetes STIGは、オペレーティングシステム、エンドポイント、アプリケーション、クラウドコンピューティングなどに対する政府レベルの防衛固有のガイダンスを備えているため、規制が厳しい環境やセキュリティの高い環境に最適です。ネットワークおよび情報セキュリティ指令（NIS2）や米国国立標準技術研究所（NIST）サイバーセキュリティ フレームワーク（CSF）などのより広範なフレームワークは、高レベルで原則に基づいています。これらは、一般的なサイバーセキュリティ戦略に対応し、包括的なガバナンスを提供する上で非常に貴重ですが、コンテナセキュリティのきめ細かな要件には対応できないため、特定の脅威ベクターを軽減することはできません。

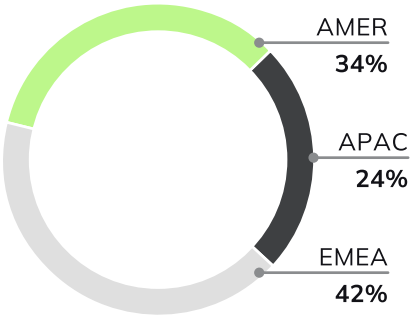
> 当社では、DISA STIGを使用してKubernetesクラウド環境のセキュリティプラクティスを実践しています。その理由としては、DISA STIGが包括的であること、頻繁に更新されていること、そしてNIST 800 53などのような当社が準拠する必要のある広範なコンプライアンスポリシーの基礎となっていることが挙げられます。
>
> - ヘルスケアIT組織、シニアインフラストラクチャーセキュリティエンジニア

最初にコンテナレベルでセキュリティを優先し、その後、規制ベンチマークに記載されているような義務付けられた戦略的セキュリティプロセスを補完することで、組織はメリットを得ることが判明しました。高度な技術を持つユーザーやセキュリティコンプライアンスを維持しているユーザーは、Kubernetesのセキュリティポスチャーをより大きな視点で捉えられる可能性が高いため、これは理にかなっています。

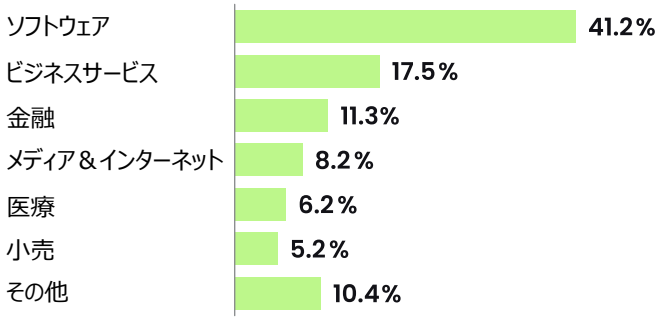
さらに、この調査では、欧州連合（EU）内で事業を展開している企業や組織は、世界で最も厳格な国際データ、プライバシー、サイバーセキュリティ規制のいくつかに準拠する必要があることが判明しました。これが、当社のデータ分析でEUを拠点とする組織がコンプライアンスポリシーをより多く採用しているように見える理由かもしれません。たとえば、主要なCSPごとにCISベンチマークの統計をサンプリングしたところ、以下の結果から、ヨーロッパ、中東、アフリカ（EMEA）の組織は他の地域よりもこれらのポリシーを有効にする傾向があることが分かります。これは、他のポリシーの大半にも当てはまります。

CIS AWS

地域

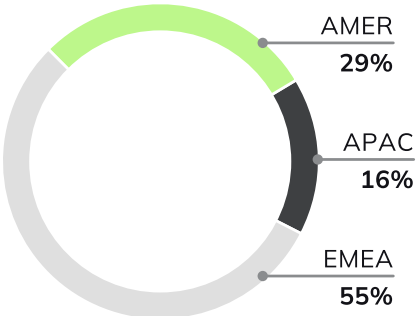


業種

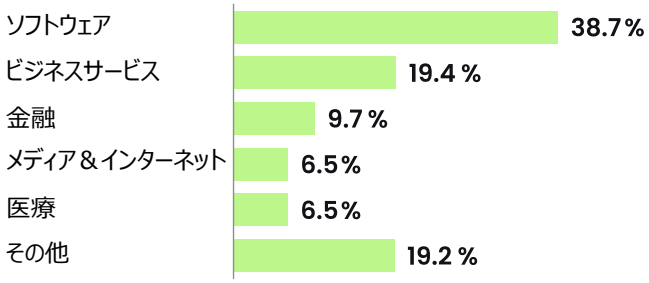


CIS GCP

地域

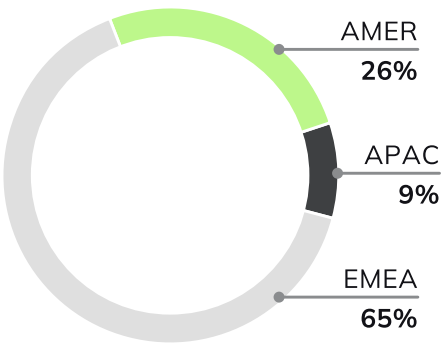


業種

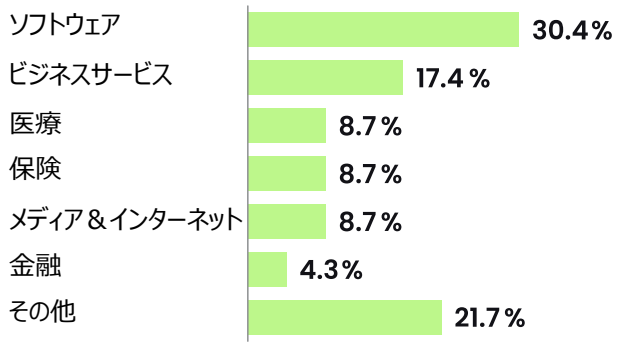


CIS Azure

地域



業種



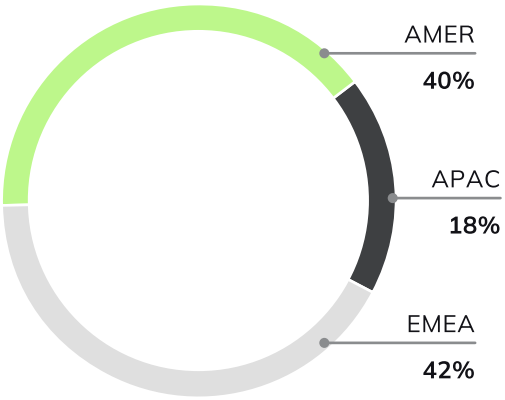
調査方法

このレポートのデータは、Sysdigのお客様が毎日稼働させ、保護している何百万件ものクラウドアカウントとKubernetesコンテナを注意深く系統的に分析して得られたものです。また、データの収集と相互関連付けを容易にするオープンソースプロジェクトの使用状況分析プラットフォームであるScarfも使用しました。本レポートの作成にあたって、当社は、世界中のクラウドに精通した広範な業界から代表的なサンプルを抽出しました。調査対象となった企業や組織は、規模もセキュリティの成熟度もさまざまであり、これにはセキュリティに関して初期段階にあるスタートアップ企業から、セキュリティポスチャーを確立している多国籍企業に至るまでが含まれています。

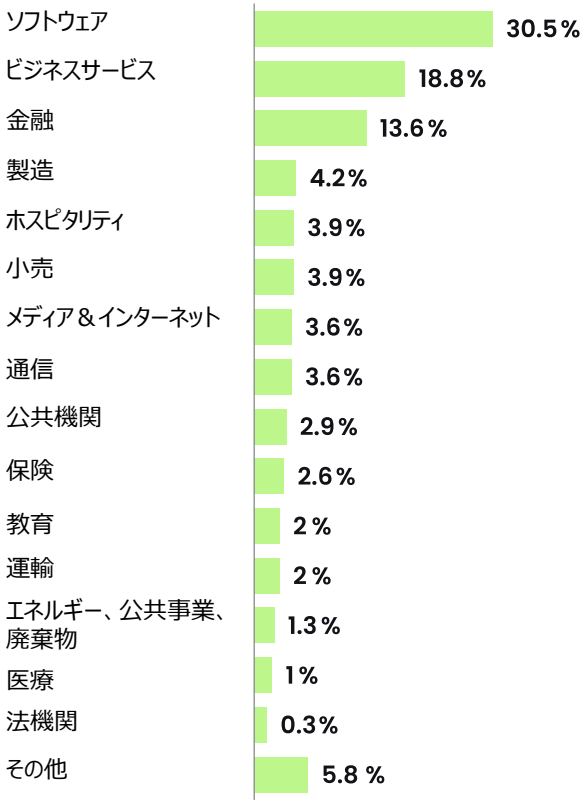
Sysdigは、Wireshark、Falco、そして最近ではStratosharkに端を発するオープンソースのルーツを持ち、情報共有と現実世界のデータに熱心に取り組んでいます。このレポートの概念と分析は、組織全体にわたる視点を持つエンジニア、製品マネージャー、脅威研究者、マーケティング担当者、および幹部からの得られたインサイトの集大成となるものであり、本レポートを読むことで、読者は、クラウド、コンテナ、セキュリティトレンドが実際どのように変化しているかを理解できます。

データの収集元

地域



業種



結論

クラウド攻撃の驚異的なスピードから、Falcoのようなオープンソースツールへの広範な依存に至るまで、Sysdigの『2025年度版クラウドネイティブセキュリティおよび使用状況レポート』は、進化し続けるクラウドセキュリティとコンテナの使用状況の貴重なスナップショットを提供します。本レポートの調査結果を導き出すために使用された実際のデータは、今後1年間の最新のクラウド環境の課題と機会を浮き彫りにします。今年の分析では、脆弱性管理とAIワークロードセキュリティ分野における大きな意味を持つ進歩が強調されたほか、サービスとユーザーアカウント間の驚くべき不均衡が明らかになりました。

企業や組織が今後12か月間に適応し、成長を続けて行くことを目指す中で、本レポートは、クラウドネイティブ環境の持つ複雑さを乗り越えるためのベンチマークとロードマップの両方として役立ちます。この目的を達成するために、オープンソースソフトウェアは、大企業と中小企業間のギャップを埋めるクラウドセキュリティの礎として確固たる地位を築いています。それでは、来年の『クラウドネイティブセキュリティおよび使用状況レポート』でまたお会いしましょう。読者の皆様が引き続き良い仕事をお続けになり、ご自分のクラウド環境を秒単位で保護されることをお祈りします。

sysdig SECURE EVERY SECOND.

クラウド環境では、1秒1秒が重要となります。攻撃は驚くほどの速さで進行するため、セキュリティチームはビジネスを減速させることなく、攻撃から守る必要があります。Sysdigは、ランタイムインサイトとオープンソースのFalcoを利用することで、リスクにおける変化を即座に検知し、クラウド攻撃をリアルタイムで阻止します。Sysdigは、クラウドのワークロード、アイデンティティ、サービス全体におけるシグナルを相互に関連付けることで、隠れた攻撃経路を明らかにすると共に、真のリスクに優先順位を付けます。予防から防御に至るまで、Sysdigは企業がイノベーションという最重要事項に集中できるよう支援します。

Sysdig. Secure Every Second.

詳細はこちら →

https://sysdig.jp

RP-011-JA REV. A 03/25