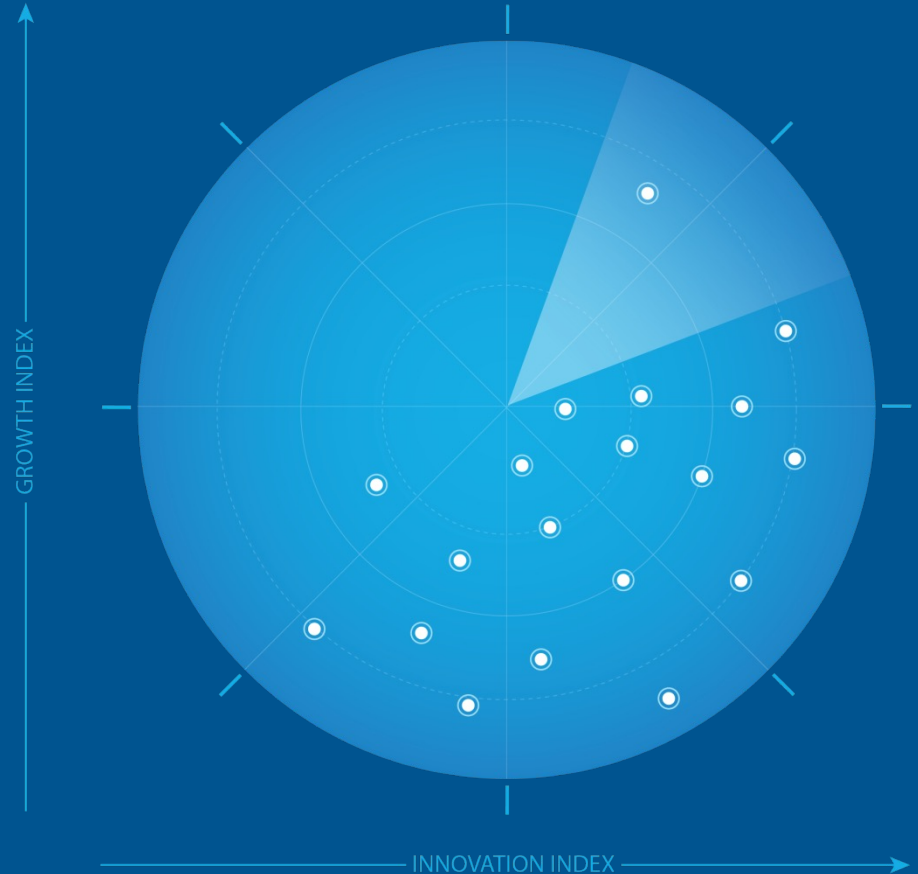


# Frost Radar™: 2022年版 クラウドネイティブ・ アプリケーション保護 プラットフォーム

企業の行動を促すベンチ  
マークシステム - 新しい取引  
フローと成長パイプライン  
を促進するイノベーション



著者 : Anh Tien Vu  
Industry Principal, Global Cybersecurity

PD8C-74  
2022年11月

FROST & SULLIVAN

# 戦略的に不可欠な要素 と成長環境





# 戦略的に不可欠な要素

クラウドコンピューティングは、さまざまなクラウドモデルとサービスを利用できるビジネス環境の標準になりつつあります。クラウドへの移行が加速したことで、企業はデジタルトランスフォーメーションに取り組み、ITインフラストラクチャとその運用を簡素化できるようになりました。

クラウドコンピューティングの使用が変えているのは、アプリケーション開発のライフサイクル、セキュリティ運用だけでなく、組織がコンテナ/Kubernetes、サーバーレス、コードとしてのインフラストラクチャ (IaC)、継続的インテグレーション/継続的デリバリー (CI/CD) プラットフォームなどのクラウド管理、アプリケーション、開発、展開のためのクラウドネイティブ技術を使用して、バックエンドインフラストラクチャ、フロントエンドにあたる顧客向けアプリケーションを構築、運用、管理する方法も変えています。

クラウドネイティブのアプリケーション開発技術にさらに焦点を当てるようになったことで、組織は従来のモノリシックアプリケーション開発モデルから、より多くのオープンソースの依存関係とライブラリを使用するマイクロサービスアーキテクチャとコンテナ化されたアプローチに移行しています。コンテナ/Kubernetes技術とサーバーレスコンピューティングはアプリケーション開発戦略を変えています。こうした技術により、組織は柔軟にアプリケーションを設計、開発、テスト、そして、市場展開できるようになったため、それに伴い、カスタマーエクスペリエンスも改善しています。[The Cloud Native Computing Foundation \(CNCF\) 2021年度調査](#)では、組織の96%がKubernetesを使用しているか、使用を検討しており、93%が現在の業務環境でコンテナを使用しているか、使用する計画があることを示しています。しかし、オープンソースソフトウェア、ライブラリ/依存関係、レジストリの使用は、これらのアプリケーションアーティファクトがコンテナイメージの脆弱性、ホストセキュリティ、コードインジェクション（サーバーレスアプリケーションの場合）、また、コンプライアンスの問題のリスクにさらされているため、これまで以上のセキュリティの脅威と懸念をもたらしています。

出典：Frost & Sullivan

# 戦略的に不可欠な要素（つづき）

ハイブリッドおよびマルチクラウド環境の複雑化と攻撃対象領域の拡大とセキュリティ運用の課題には、組織に可視性、制御、保護をもたらす、現代のクラウドコンピューティングアーキテクチャ（例：仮想マシン（VM）、コンテナ、Kubernetes、サーバーレス）を安全に運用しながら、ソフトウェア開発のライフサイクルにセキュリティを統合し、さらに、効果的にコンプライアンスに対処することを可能にする統合クラウドネイティブプラットフォームが必要です。従来のセキュリティアプローチはマイクロセグメンテーションをサポートするように設計されていないため、特にコンテナ環境やサーバーレス環境でのアプリケーションの変更に対応できるほど堅牢に設計されておらず、時代遅れになっています。

その結果、CNCFは「シフトレフトとシールドライト」セキュリティモデルへのパラダイムシフトを呼びかけました。その目的は、セキュリティをラベルやタグなどの属性とメタデータに基づいて識別される動的ワークロードに近づけることでクラウドネイティブ・アプリケーションを保護することです。このモデルでは、後半のフェーズだけでなく、アプリケーション開発ライフサイクルの初期段階から全体にわたってセキュリティを統合する必要があります。そして、アプリケーションが展開されて実行されるクラウド環境のセキュリティ管理も必要です。これにより、クラウドネイティブ・アプリケーション保護プラットフォーム（CNAPP）の必要性が拡大しています。

CNAPPがあれば、組織は、クラウドセキュリティポスチャ管理（CSPM）、クラウドワークロード保護プラットフォーム（CWPP）、脆弱性管理などのポイントセキュリティソリューションではなく、統合セキュリティプラットフォームを使用して、セキュリティの脅威と課題に対処できます。CNAPPは、セキュリティ、IT/プラットフォームと開発チーム間のより良いコラボレーションも可能にし、生産性を改善し、クラウド環境でより効率的に機能するリスク管理も可能にします。

# 成長環境

CNAPPのグローバル市場は、2021年に17億2060万ドルの収益を記録し、前年比48.8%の成長を示しました。Frost & Sullivanは、2021年から2026年にかけて年平均成長率25.7%の勢いが続き、2026年には同市場の収益は、54億680万ドルに達すると予測しています。クラウド・インフラストラクチャのセキュリティを強化し、アプリケーションとデータをライフサイクル全体で保護する、統合クラウドセキュリティプラットフォームの需要が拡大し続けているためです。

一般に、組織はかなり長い間、CNAPPコンポーネントを個別に採用してきました。その筆頭に挙げられるのは、クラウドセキュリティの可視性と制御のためのCSPMと、ランタイム保護とコンプライアンスのためのCWPPです。DevOpsセキュリティへの投資は、ソフトウェア開発ライフサイクルの初期段階にセキュリティを取り入れるためのシフトレフトセキュリティの必要性により、最近増加しています。同様に、クラウド・インフラストラクチャ・エンタイトルメント管理(CIEM)とクラウド・ネットワーク・セキュリティは、クラウドサービス・プロバイダが提供するクラウドネイティブソリューションを使用することで、いち早くクラウドを採用してきた企業の間で広く使用されています。

世界中の組織は、さまざまな形式のCNAPPに多額の費用を費やしています。そのほとんどは、特定のユースケースや課題に対処するための個別の製品です。こうした個々のツールを統合するというCNAPPの概念は、CNAPPという言葉同様にまだ、なじみのないものであるため、潜在的なユーザーの間で混乱が生じ、投資に対するアプローチも慎重を期したものとなります。しかしそれでも、クラウドサービスとクラウドネイティブ・アプリケーション開発技術の採用の加速と、クラウド環境での攻撃対象領域の増加により、クラウドセキュリティ・テクノロジー全体、特にCNAPPプラットフォームへの支出は増加するものと考えられます。

# 成長環境（つづき）

多くの組織、特に成熟した組織は、サイロ化されたアプリケーションのリスク、オープンソースのリスク、インフラストラクチャとワークロードが直面している脅威に迅速に対応できないことが、チームにセキュリティのギャップと複雑さをもたらす可能性があることを理解しています。一元化されたビューでリスクを特定し、優先順位を付け、修復する必要性により、**CNAPP**の需要が高まります。

セキュリティとコンプライアンスのリスクを一緒に管理するためには、より優れたセキュリティ保護、詳細な可視性、リスク管理の効率性を提供する単一のプラットフォームが必要です。これには、マルチクラウド戦略採用の増加、ワークロードを攻撃から保護する継続的な必要性、そして、クラウド・インフラストラクチャ、コンテナ/Kubernetes、IaC、またはCI/CDパイプラインなど、さまざまな環境全体で一貫したポリシーの適用を一元化するというプレッシャーが伴います。

ソフトウェア構築のすべての段階（開発、テスト、リリース）で設計によるセキュリティ（シフトレフトセキュリティ）を有効にするため、**CNAPP**をDevOpsソフトウェア開発ライフサイクルフレームワークおよびCI/CDパイプラインプラットフォームとより適切に統合する必要性は拡大しています。

**CNAPP**とDevOpsの統合は、アプリケーション・アーティファクト・スキャン（静的および動的アプリケーション・セキュリティ・テスト [SAST/DAST]、アプリケーション・プログラミング・インターフェイス [API] スキャン、ソフトウェア構成分析 [SCA]、および脆弱性管理）、構成、ランタイムの動作分析、およびコンプライアンス要件に関連するクラウドのリスクに関連して生じる主な懸案事項に対処するためのものです。この推移により、クラウドネイティブプラットフォーム、特にコンテナ/Kubernetes、ホスト、アプリケーションの依存関係、サーバーレスアプリケーション/コード、CI/CD ツール、その他のオーケストレーションプラットフォームを保護するためのクラウドネイティブ・セキュリティ・ソリューションの必要性が高まっています。

# 成長環境（つづき）


消費に関して言えば、CSPM、CWPP、DevOpsセキュリティは今後もCNAPPの主要な機能ですが、CIEMとクラウド・ネットワーク・セキュリティ・サービスも今後5年間で普及するでしょう。多くの組織は、管理と保護の効率を向上させるために、1つのベンダーが提供する少なくとも2つのコンポーネントを同時に使用しているようです。

クラウドセキュリティユースケースの統一化は今後数年間継続し、より多くのベンダーが、独自の技術または買収を通じてCNAPP市場に参入すると予想されています。Kaspersky、Fortinet、VMwareなど強力なCWPP製品を有する企業は、技術の拡張または買収を通じて市場に参入する公算が大きくなっています。それでもなお、市場では、CSPM、CWPP、DevOpsセキュリティに焦点を当てた独自のクラウドネイティブ・セキュリティ・ソリューションを備えた新興企業による、より革新的な開発と競争が見られる可能性があります。

この独立分析に関連するFrost & Sullivanの調査：

- [Global Cloud Workload Protection \(CWP\) Growth Opportunities](#)
- [Global Cloud-native Application Protection Platform Growth Opportunities, 2022](#)



F R O S T  S U L L I V A N

## Frost Radar™

クラウドネイティブ・  
アプリケーション保護  
プラットフォーム

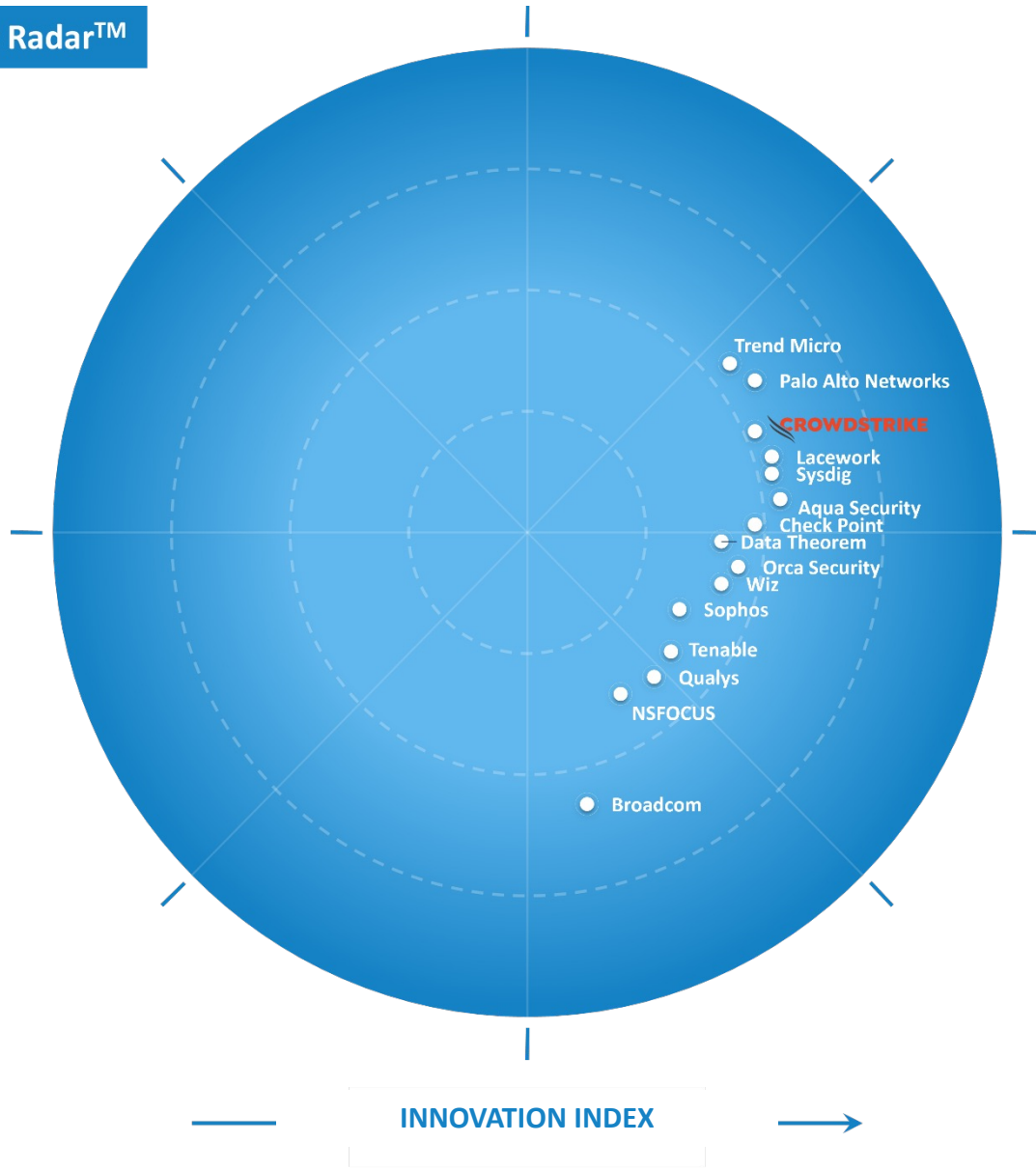




# Frost Radar™: クラウドネイティブ・アプリケーション保護プラットフォーム

Frost Radar™

GROWTH INDEX



INNOVATION INDEX

出典 : Frost & Sullivan

CNAPP市場は、従来のネットワークおよびエンドポイントセキュリティベンダー、脆弱性評価ベンダー、クラウドセキュリティを専門とする新興企業の参加により、比較的初期段階にあり、断片化されたままでした。世界中で20を超える業界参加企業から、Frost & Sullivanは独自のFrost Radar™分析で上位15社を精査しました。本レポートに含まれるベンダーは以下の条件を満たします：

- 2021年および2022年前半に2つ以上の地域（北米、ヨーロッパ、中東、アフリカ [EMEA]、アジア太平洋 [APAC]、中南米）でプレゼンスを持つ
- 2021年の年間収益が2,000万ドル以上で、少なくとも1%のマーケットシェアを持つ
- 2022年9月までに認められたCNAPPプラットフォームがある（すなわち、少なくともCSPMおよびCWPP機能が含まれるプラットフォーム）。

今回のFrost Radar™で取り上げる企業は以下のとおりです：Aqua Security、Broadcom、Check Point Software Technologies、CrowdStrike、Data Theorem、Lacework、NSFOCUS、Orca Security、Palo Alto Networks、Qualys、Sophos、Sysdig、Tenable、Trend Micro、Wiz。

他の企業も市場調査中か、最近参入していますが、Frost & Sullivanは上記の企業がCNAPP市場を支配、形成している原動力であると特定しました。

市場が進化し続ける中、より多くの大規模なサイバーセキュリティ企業やクラウドセキュリティの新興企業が市場に参入するでしょう。Frost & Sullivanは、市場の競争がさらに激化し、市場参入戦略と技術革新の両方の観点から、今後数年間で状況が大きく変化すると考えています。

## 市場競争激化の環境（つづき）

企業がセキュリティ体制を管理し、クラウドネイティブ環境でのアプリケーション開発ライフサイクル全体にわたってセキュリティリスクと脅威を検知、対応できるようにセキュリティ機能を統合し、連携させる統合プラットフォームを提供するベンダーの能力こそ、顧客の意思決定プロセスにおける主な要因ですが、併せて強力なサポート体制、手頃な価格、柔軟で透明性の高い価格体系なども重要な要因です。

顧客は、ビルドから本番まで、DevOps、DevSecOps、そしてクラウド・インフラストラクチャの全体で可視性とセキュリティを提供できる、より広範な機能セットを求めています。これは、顧客がスタック全体（コード、アプリケーション、ワークロード、インフラストラクチャ）をカバーするCNAPPソリューションを求めているということに他なりません。実際、こうしたソリューションは包括的なセキュリティ戦略を実現し、さまざまなクラウド環境でゼロトラストセキュリティに到達する上で役立ちます。

組織は、人工知能/機械学習（AI/ML）機能をますます活用して、クラウド環境でのリスクをより適切に管理しているため、CNAPPソリューションは、シフトレフトしてコードの開始と開発の初期段階でAIとMLを組み込む必要があります。これは、ワークロード/アプリケーションの振舞いとクラウド・インフラストラクチャ内でそれぞれがどう関与するかについての、より優れたインサイトを取得することで、自動化された脅威検知と対応機能を増加するためです。

Webアプリケーション保護とのより強力な統合に対する需要が高まっています。それは保護を、それらの基盤となるクラウドワークロードの保護と統合する必要があるためです。



## 市場競争激化の環境（つづき）

CNAPPは、自己ホスト型、マネージド・セキュリティ・サービス・プロバイダーのパートナーシップを通じて管理されるもの、またはソフトウェア・アズ・ア・サービス（SaaS）として利用できますが、顧客は、オーバーヘッドを削減し、リソースを再割り当てし、信頼性を高めるために、クラウド配信モデルを選択する傾向があります。特に、中小企業に至ってはその傾向が強くなります。しかし、大企業や規制管理の厳しい業界の場合、プライバシーとコンプライアンスの要件が課せられているため、自己ホスト型モデルが検討されることも多々あるでしょう。

クラウドストライクは、マーケットシェアは7位にとどまっているにもかかわらず、過去3年間にわたり、強力で一貫した成長を遂げたため成長インデックスに選ばれました。Frost & Sullivanは、同社の強力な顧客基盤とより優れたブランド認知度、および同社のクラウドセキュリティへの注力を認識しており、こうした要因に基づきクラウドストライクは、今後2～3年にわたりCNAPPの堅調な成長の勢いを維持すると考えられています。

## **Company to Action:**

投資、パートナーシップ、ベンチマークに  
あたり最初に検討すべき企業

# クラウドストライク

## イノベーション

- クラウドストライクのCNAPP製品は、エージェントベースのFalcon Cloud Workload Protection、エージェントレスのFalcon Horizon (CSPM)、CIEM、およびシフトレフト・セキュリティ・モデルに拡張されたコンテナセキュリティで構成され、包括的なCrowdStrike Falconプラットフォームの一部として提供されています。
- このプラットフォームは、マルウェア以外の脅威やファイルレス攻撃の検知に振舞い分析技術を使用します。早期の脆弱性特定、脅威の検知と対応、ランタイム保護、コンプライアンスの実施を通して、企業がクラウドの構成ミスを検出、防止し、コンプライアンスを確保し、ホスト、VM、アプリケーション、コンテナ/Kubernetesを管理、保護します。これらの機能は2つの個別のモジュールで提供されるものの、両方ともに、エンドポイント、クラウドワークロード、コンテナ、およびその他のテレメトリソースから収集された独自のThreat Graph、Asset Graph、Intel Graphデータベースを備えたCrowdStrike Falconを介して提供されます。

## 成長

- クラウドストライクは急成長しているクラウドセキュリティベンダーの一社で、主に同社のXDR/EDR、MDRソリューションがその成長を促進しています。同社のCNAPPビジネスは、同社がクラウドセキュリティ市場により重点を置いていることを示していることから、世界的に注目を集めています。
- Frost & Sullivanの予測に基づけば、クラウドストライクのCNAPP収益は2021年に前年比成長率71.7%を記録し、5.0%のマーケットシェアを獲得し、市場の主要ベンダーの一社になりました。
- 地理的には、同社の主な取引は北米ですが、EMEAでの前年比成長率は92.6%、APACでは82.3%となっています。
- 強力なチャネルパートナーエコシステムを備えた急成長中のクラウドネイティブ・エンドポイント・セキュリティ・ベンダーの一社であるクラウドストライクは、クラウドセキュリティモジュールを様々な業種の大企業にクロスセルおよびアップセルすることが可能であり、この点は同社の強力な成長の勢いを今後も後押しするものと見られます。

## FROSTの展望

- クラウドストライクは、同社が提供するCNAPP製品により、この数年間に世界中で急速な成長を達成しました。
- Frost & Sullivanは、持続可能なパイプライン、XDR/EDR製品による強力な顧客基盤、強力なチャネルパートナー・エコシステムを通じた同社の成長の勢いを認識しており、こうした同社の特色は、今後もCNAPPビジネスの前進を推進するものと考えられます。
- 特に、MDRサービスおよびクラウド脅威ハンティングサービスの提供は、顧客の信頼を高め、ソリューションを使用する際のエクスペリエンスを向上させるのに役立つため、競合他社との差別化セールスポイントと見なせます。
- こうした状況にあっても、クラウドストライクは、CWPPではなく、CSPMやCIEMなど他の機能を使用して、CNAPPソリューションのユースケースを多様化する必要があります。さらに、プラットフォームをより包括的にするために、コード脆弱性スキャン機能を搭載しCNAPP製品を拡張すべきであると言えます。

出典：Frost & Sullivan



FROST & SULLIVAN

戦略的  
インサイト



# 戦略的インサイト

1

CNAPP市場はまだ黎明期にあるものの、今後2年から3年間に参入するベンダーが増えることから、競争が激化しています。これは、技術革新と価格体系の両方で競争力を維持する上で、既存のベンダーに大きな負担と圧力をかけることとなります。激しい競争により、同市場に参入している企業各社はR&DおよびM&A活動により多くの労力を払い、プラットフォーム機能を強化して牽引力を得て、総所有コストを削減する方法を見つけながら、顧客により良いサポートとエクスペリエンスを提供できるようにする必要が生じてくるものとみられます。

2

現在初期段階にあるCNAPP市場の成功のためには、マーケットに対する教育が重要です。ベンダーは、業界関係者と緊密に連携して、世界的企業にクラウドセキュリティの認識を高め、クラウドソリューション導入までの過程におけるCNAPPコンセプトの重要性を強化することが不可欠でしょう。ベンダーの成長はチャネルパートナープログラムに大きく左右されます。そのため、ベンダーにとっては、マーケットに対する教育やソリューションの宣伝を支援し、さらに、クライアントのエンゲージメントを図り、顧客の信頼を得て、顧客の要望の理解の一助となるローカルサポートを提供可能な適切なチャネルパートナーの存在は不可欠です。

3

CNAPPの選択と導入はCISO単独の決定ではありません。CNAPPには、さまざまな開発、セキュリティ、運用チームが関与し、それぞれに独自の戦略、希望、重要業績評価指標があるため、全面的で緊密なコラボレーションが必要となります。この決定には、最高情報責任者、主任開発者、およびビジネスリーダーからの意見も考慮する必要があります。こうした関係者全員が共通の目標を達成したいと考えているためです。

出典：Frost & Sullivan



次のステップ：  
Frost Radar™を活用して  
主なステークホルダーを  
支援





# Frost Radar™で取り上げられることの意義

---

Frost Radar™で取り上げられた企業は、業界の成長、イノベーション、またはその両方におけるリーダーであり、業界が将来発展する上で欠かせない存在です。

---

## 成長の可能性

貴社は将来的に大きな成長の可能性があるため、「Company to Action」に取り上げられました。

## ベストプラクティス

貴社は業界内でGrowth Pipeline™のベストプラクティスを形成するのに適した位置づけです。

## 競争の激しさ

貴社は、この成長環境における競争激化の主要な推進企業の一社です。

## カスタムバリュー

貴社は顧客へのバリュープロポジションを大幅に高める能力を実証してきました。

## パートナーとしての潜在性

貴社は、顧客、投資家、バリューチェーンパートナー、そして将来の人材から重要な価値提供者として最優先に位置づけられています。

出典：Frost & Sullivan

# Frost Radar™はCEOの成長チームを支援

## 戦略的に不可欠な要素

- 成長を達成することはますます困難になっています。
- 競争の激しさが増す一方です。
- より多くのコラボレーション、チームワーク、そしてフォーカスが必要です。
- 成長環境は複雑です。

## FROST RADAR™の活用

- Growth Teamには、経営陣全体で協力的な環境を促進し、ベストプラクティスを推進するために必要なツールがあります。
- Growth Teamには将来の成長可能性を評価するための測定プラットフォームがあります。
- Growth Teamには強力なGrowth Pipeline™でCEOをサポートする能力があります。

## 次のステップ

- **Growth Pipeline Audit™**
- **Growth Pipeline as a Service™**
- **Growth Pipeline™ Dialogue with Team Frost**

出典：Frost & Sullivan

# Frost Radar™は投資家を支援

## 戦略的に不可欠な要素

- 取引フローは減少、競争は劇化。
- デューデリジェンスは業界の複雑さによって妨げられています。
- ポートフォリオ管理は効果的ではありません。

## FROST RADAR™の活用

- 潜在性の高い投資に対して行動する企業の強力なパイプラインを作成することによって、投資家は将来の成長可能性にフォーカスできます。
- 投資家は正確さを高め、取引プロセスを加速するデューデリジェンスを実行できます。
- 投資家は最大の内部収益率を実現し、株主の長期的な成功を確保できます。
- 投資家は、最適なポートフォリオ管理のためのベストプラクティスを使用して、パフォーマンスを継続的にベンチマークできます。

## 次のステップ

- **Growth Pipeline™ Dialogue**
- **Opportunity Universe Workshop**
- **Growth Pipeline Audit™ as Mandated Due Diligence**

出典：Frost & Sullivan

# Frost Radar™は顧客を支援

## 戦略的に不可欠な要素

- ソリューションはますます複雑化し、長期的な影響が発生します。
- ベンダーソリューションはわかりづらいこともあります。
- ベンダーの変動はさらに不確実性を増します。

## FROST RADAR™の活用

- 顧客は、潜在的なベンダーを評価し、強力で長期的なソリューションを提供するパートナーを特定するための分析フレームワークを持っています。
- 顧客は、最も革新的なソリューションを評価し、個々のソリューションがニーズをどのように満たすかを理解できます。
- 顧客は、ベンダーパートナーシップに関して長期的な視点を得ることができます。

## 次のステップ

- **Growth Pipeline™ Dialogue**
- **Growth Pipeline™ Diagnostic**
- **Frost Radar™ Benchmarking System**

出典：Frost & Sullivan



# Frost Radar™は取締役会を支援

## 戦略的に不可欠な要素

- 成長はますます困難になっています。CEOはガイダンスが必要です。
- 成長環境には複雑な先導スキルが必要です。
- 顧客バリューチェーンは変動しています。

## FROST RADAR™の活用

- 取締役会には、企業の長期的な成功を確実に監視する独自の測定システムがあります。
- 取締役会には、株主の投資を保護することにつながる、問題解決、ベンチマーク、ベストプラクティスを中心としたディスカッションプラットフォームがあります。
- 取締役会は、将来の成長の可能性を最大化するための、CEOへの巧みなメンタリング、サポート、ガバナンスを確保することができます。

## 次のステップ

- **Growth Pipeline Audit™**
- **Growth Pipeline as a Service™**

出典：Frost & Sullivan

FROST & SULLIVAN

# Frost Radar™ Analytics



# Frost Radar™: 将来の成長の可能性をベンチマーク化

## 2つの主要インデックス、10の分析材料、1つのプラットフォーム

### GROWTH INDEX（成長指数）の要素

#### 縦軸

**GROWTH INDEX (GI)**、成長指数は、企業の成長パフォーマンスと実績、さらに完全に足並みをそろえたビジョンと成長戦略 - 堅牢な成長パイプラインシステム、効果的な市場、競合他社、エンドユーザーに焦点を当てた販売およびマーケティング戦略 - を開発および実行する能力の尺度です。

- **GI1: マーケットシェア（過去3年間）**  
過去3年間の特定の市場における企業のマーケットシェアを競合他社と比較したものです。
- **GI2: 収益の伸び（過去3年間）**  
特定のFrost Radar™のコンテキストを形成する市場/業界/カテゴリにおける、過去3年間の企業の収益成長率を示します。
- **GI3: 成長パイプライン**  
これは、企業の成長パイプラインシステムの強さと活用の度合いを評価して、成長機会の状況を継続的に把握、分析し、優先順位を付けたものです。
- **GI4: ビジョンと戦略**  
企業の成長戦略がそのビジョンとどの程度一致しているかを評価するものです。企業が行っている新製品や新市場への投資は、同社が示すビジョンと一致していますか？
- **GI5: セールスとマーケティング**  
需要を促進し、成長目標を達成するのに役立つ、企業のセールスとマーケティング活動の有効性の尺度です。



# Frost Radar™: 将来の成長の可能性をベンチマーク化

## 2つの主要インデックス、10の分析材料、1つのプラットフォーム

### 横軸

**INNOVATION INDEX (II)** は、製品/サービス/ソリューションを開発する企業の能力の尺度です - グローバルに適用可能であり、複数の市場にサービスを提供するために進化および拡大可能で、顧客ニーズの変化に合わせた、破壊的なメガトレンドを明確に理解した製品/サービス/ソリューション

### INNOVATION INDEXの要素

- **II1: イノベーションスケラビリティ**  
組織のイノベーションがグローバルに拡張可能であり、発展途上市場と成熟市場の両方で適用可能であるかどうか、また隣接する業界と隣接していない業界にも適用できるかがを判断するものです。
- **II2: 研究開発**  
企業のR&D戦略の有効性の尺度であり、R&D投資の規模とイノベーションパイプラインをどう満たすかによって決定されます。
- **II3: 製品ポートフォリオ**  
企業の製品ポートフォリオの尺度であり、年間収益に対する新製品の相対的な割合に焦点を当てています。
- **II4: メガトレンドの活用**  
イノベーションパイプラインの基盤として、企業が進化、長期的な機会、新しいビジネスモデルを積極的に活用しているかどうかを評価するものです。メガトレンドの説明は[こちら](#)をご覧ください。
- **II5: カスタマーアライメント**  
企業の製品/サービス/ソリューションの、現在および潜在的な顧客への適用可能性と、変化する顧客のニーズによって同社のイノベーション戦略がどのように影響を受けているかを評価します。



# 參考資料

# 略語一覧

**CNAPP: Cloud Native Application Protection Platform** (クラウドネイティブ・アプリケーション保護プラットフォーム)

**DAST: Dynamic Application Security Testing** (動的アプリケーションセキュリティテスト)

**IAST: Interactive Application Security Testing** (インタラクティブ・アプリケーション・セキュリティ・テスト)

**SAST: Static Application Security Testing** (静的アプリケーションセキュリティテスト)

**CSPM: Cloud Security Posture Management** (クラウドセキュリティポスチャ管理)

**CWPP: Cloud Workload Protection Platform** (クラウドワークロード保護プラットフォーム)

**IaC: Infrastructure as Code** (インフラストラクチャ・アズ・ア・コード)

**CIEM: Cloud Infrastructure Entitlement Management** (クラウド・インフラストラクチャ権限管理)

**CI/CD: Continuous Integration / Continuous Delivery** (継続的インテグレーション/継続的デリバリ)

**API: Application Program Interface** (アプリケーション・プログラム・インターフェース)

**SCA: Software Composition Analysis** (ソフトウェアコンポジション解析)

**SBOM: Software Bill of Materials** (ソフトウェア部品表)

**CNWS: Cloud Networks Security** (クラウド・ネットワーク・セキュリティ)

**WAAP: Web Application and API Protection** (WebアプリケーションとAPI保護)



# 法的免責事項

Frost & Sullivanは、企業またはユーザーから提供された不正確な情報について責任を負いません。定量的な市場情報は、主に聞き取りに基づいており、変動する可能性があります。Frost & Sullivanの調査サービスは、選択された一部の顧客グループに提供される貴重な市場情報を含む限定刊行物です。顧客は、注文またはダウンロードの際に、Frost & Sullivanの調査サービスが社内利用目的であり、一般公開または第三者への開示のためのものではないことに同意します。本調査サービスのいかなる部分も、当社からの書面による許可なく、顧客以外に提供、貸与、転売、または開示することはできません。さらに、発行者の許可なしに、電子的、機械的、写真複製、録音、またはその他のいかなる形式や手段によっても、本調査のいかなる部分も複製したり、情報検索システムに保存または送信することはできません。

許可に関する詳細情報はこちらまでお問合せください：[permission@frost.com](mailto:permission@frost.com)

© 2022 Frost & Sullivan. 無断複製禁止。本書は機密情報が含まれる、Frost & Sullivanの専有物です。  
Frost & Sullivanの書面による承諾なく、本書のいかなる部分も配布、引用、コピー、またはその他の方法で複製することはできません。