protiviti®
Global Business Consulting

CNAPPでクラウド環境を保護する

2023年、ある世界的な大手テクノロジー企業が重大なセキュリティ侵害に見舞われました。これは、機密性の高い本番データが誤って開発環境に復元されたことによるものでした。この設定ミスにより、認証情報や顧客データが流出し、最先端のテクノロジー企業であってもクラウド環境のセキュリティ確保に依然として課題があることが浮き彫りになりました。

このようなインシデントは決して珍しいものではありません。ガートナー社によると、2023年までにクラウドセキュリティの障害の75%は、セキュリティ設定の誤りに起因すると報告されています。これらの失敗の主な原因には、セキュリティツールの連携不足、事後対応型のセキュリティ戦略、クラウド環境全体における統一された可視性の欠如などが挙げられます。これらの問題は、統合的かつ積極的なセキュリティ対策の必要性を浮き彫りにしています。

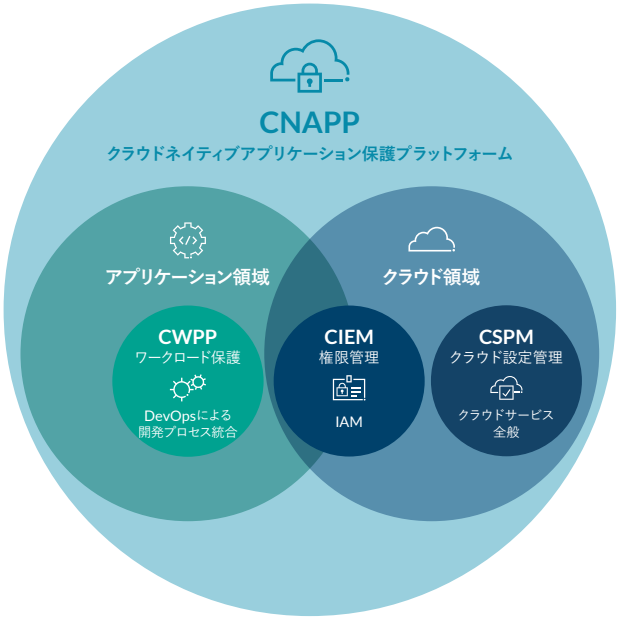
セキュリティチームの多くでは、Splunkなどのセキュリティ情報およびイベント管理（SEIM）システムや、CrowdStrike Falconなどのエンドポイント検出対応（EDR）ツールに依存しています。これらのソリューションは、一元化されたログ管理とリアルタイムの脅威検出機能を提供しますが、クラウドネイティブ環境特有の速度、規模、複雑さに対応するには不十分な場合が多くあります。

そこで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）の出番です。CNAPPは、セキュリティとコンプライアンスを1つのプラットフォームに統合し、クラウドセキュリティに対する統合的で積極的なアプローチを提供します。サイロ化して動作する従来のツールとは異なり、CNAPPは継続的なモニタリングとガバナンスを提供し、開発、運用、セキュリティの各チームが連携して、最新のアプリケーションのライフサイクル全体にわたるリスクに対処します。

巧妙化するサイバー攻撃

今日の企業環境では、サイバー脅威と攻撃の頻度と高度化が進んでいるため、CNAPPは単なる贅沢品ではなく、必需品になりつつあります。クラウドネイティブアプリケーションの開発が拡大し、サイバー攻撃の脅威がより巧妙になる中、CNAPPは、現代の企業が貴重な資産を保護するために必要な、包括的で統合されたセキュリティソリューションを提供します。

CNAPPにつながるクラウドセキュリティの進化は、クラウドネイティブテクノロジーの急速な開発手法に対応できる、よりダイナミックでスケーラブルなセキュリティソリューションへの移行を反映しています。組織がマルチクラウド環境を採用し続ける中、堅牢で統合されたセキュリティプラットフォームの必要性がますます高まっています。企業のセキュリティの未来は、CNAPPを導入することで、組織がクラウド上で安全にイノベーションとスケールアップを実現できるようになります。



「組織のクラウド環境が年々複雑化する中、クラウドにおける脅威や脆弱性の監視、検出、防止もさらに大きな課題となっています。セキュリティツールの普及と断片化も相まって、セキュリティチームはクラウド環境のセキュリティ確保においてこれまで以上に複雑な課題に直面しています。複数のクラウドプラットフォームに包括的で統合されたセキュリティを提供する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）が、なぜ業界で急速に人気を集めているのかは、容易に理解できます。」

ヒラリー・バロン
シニアテクニカルディレクター、リサーチ クラウドセキュリティアライアンス

CNAPPの役割を理解する

従来のセキュリティソリューション —SIEM、ファイアウォール、エンドポイント検出などの従来型のセキュリティソリューション —は、ログを監視し、インシデント発生後に脅威を検知することに優れています。しかし、これらのソリューションは、クラウドネイティブな処理負荷やKubernetesクラスタ、ダイナミックで自動スケーリング可能なインフラ向けに構築されたものではありません。

従来のセキュリティツールと比較して、CNAPPはどのようにこれらの課題に対処しているのでしょう。

機能	従来型セキュリティ（SIEM、ファイアウォール、EDR）	CNAPP
脅威検出	過去のデータログを調べて、 セキュリティ侵害が発生した後に検出	セキュリティをリアルタイムで監視し、 侵害される前にリスクを特定
脅威対応	セキュリティアラートを送信し、 手動で調査・修正が必要	問題を自動で修正し、 被害を未然に防ぐ
脅威防御	コンピュータ、社内ネットワーク、 従来型サーバーを保護	クラウドアプリ、コンテナ、 およびサーバーレスコンピューティングを保護
モダンアプリケーション開発	ソフトウェア開発後にセキュリティを追加するため、 問題の発見が遅れる	ソフトフェア開発プロセスに組み込み、 セキュリティ問題を事前に防止
コンプライアンス	セキュリティチームが手動で監査を行い、 ルール遵守を確認	セキュリティ規則の遵守をリアルタイムで 自動的に確認し、手作業による労力を軽減

図1：従来型セキュリティとCNAPPの比較

重要なポイント：CNAPPは、SIEMやEDRに取って代わるものではなく、これらの従来型ツールが現代のクラウド環境で見逃しがちなセキュリティギャップを埋める役割を果たします。

CNAPPはどのように現実のクラウドセキュリティの課題を解決しているのでしょうか。

- **セキュリティの脅威を未然に防ぐ（シフトレフトセキュリティ）**：ある金融サービス企業は、誤った設定のストレージバケットによって機密データが漏洩するという問題に直面しました。この組織のSIEMシステムはアラートで通知しましたが、それは漏洩がすでに発生した後でした。CNAPPのシフトレフトアプローチを採用することで、同社は運用前にセキュリティチェックを実装し、設定ミスが脅威となる前に検出できるようになりました。

  成果：脅威の事前防止とセキュリティ態勢の強化。

- **ツールの乱立を減らし、セキュリティ体制を強化する**：セキュリティチームは、マルチクラウド環境のセキュリティを確保するために10以上のツールを管理することが多く、その結果、見落としやアラートの重複、運用の非効率性につながっています。あるグローバル企業は、CNAPPを使用してセキュリティスタックを統合し、脅威検出の精度を向上させながら、ツール数を60%削減しました。

  成果：アラートの減少、可視性の向上、対応時間の短縮。

- **AIによる脅威検知—チームを増員することなくセキュリティを拡張する**：小規模なセキュリティチームを抱えるあるクライアントは、設定ミスやID関連の脅威への対応に苦労していました。AIを活用した分析機能を持つCNAPPを採用することで、アナリストを増員することなく、設定ミスの検出とポリシー施行を自動化することができました。

  成果：脅威の検出が40%高速化し、手作業による作業負荷が軽減。

これらの例は、CNAPPがどのようにクラウドセキュリティの重要な課題に対処し、クラウド環境を保護するためのより効率的で効果的なアプローチを組織に提供しているかを示しています。

IaCセキュリティ：コードの枠を超えて

Infrastructure-as-Code（IaC）のセキュリティを検討する際、多くの組織はTerraformやCloudFormationのようなスキャンツールに注目しがちです。しかし、真のIaCセキュリティはそれ以上の範囲に及びます。CNAPPは以下のような包括的なアプローチを採用しています。

- **OSイメージと仮想マシン（VM）テンプレート**：Amazon Machine Images（AMI）とAzure VMイメージの強化版などが含まれます。
- **コンテナ設定**：KubernetesのYAMLファイルやHelmチャートをカバーします。

- **IAMポリシーとアクセス制御設定**：Amazon Web Services（AWS）のIdentityとAccess Management（IAM）やAzure Role-Based Access Control（RBAC）の設定ミスに対処します。

大手SaaSプロバイダーの社員が共有してくれた経験によると、不適切なKubernetesのデプロイメントYAMLにより、アプリケーションのワークロードに過剰な権限が付与されていたケースがありました。同組織のSIEMはこの問題を検出できませんでしたが、CNAPPは運用前にこの設定ミスを検出してブロックし、堅牢なIaCセキュリティの確保における有効性を示しました。

> 「セキュリティチームは、Splunkのようなセキュリティ情報イベント管理システム（SIEM）や、エンドポイント検出および対応ツール（EDR）に依存することが多いのですが、これらのソリューションは、クラウドネイティブ環境のスピード、スケール、複雑性に対応できるようには構築されていません。そこで登場するのが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）です。従来型のツールでは難しかった統合的かつ積極的なクラウドセキュリティアプローチを提供します。」
>
> スティーブン・サルゴン
> プロティビティ、マネージャー、エンタープライズクラウド、
> テクノロジーコンサルティング

CNAPPの効果的な導入

CNAPPを採用することは、単に新しいセキュリティツールを導入することではなく、クラウドにおけるサイバーセキュリティへの組織の取り組み方の根本的な変革を意味します。この変革には、セキュリティ対策をクラウドネイティブ環境にシームレスに統合することに焦点を当てた、積極的な考え方が必要です。ここでは、組織がCNAPPを効果的に導入する方法を紹介します。

- **クラウドセキュリティ態勢の評価**：現在のクラウドインフラストラクチャの脆弱性やコンプライアンスギャップを評価することで、設定ミスやリスクを特定します。
- **DevSecOpsとの統合**：セキュリティ対策をCI/CDプロセスに組み込み、問題に早期に対処します。
- **AIと自動化の活用**：人工知能と自動化を活用した脅威検知機能の強化により、アラートの負担を軽減し、対応時間を短縮します。
- **コンプライアンスを継続的に監視**：NIST、ISO 27001、CIS、地域規制などの標準に準拠したセキュリティ監査を自動化します。
- **IAMの導入**：アクセス制御を定期的に見直し、調整することで、最小権限の原則を適用します。
- **IaCセキュリティの活用**：導入前にIaCテンプレートの脆弱性をスキャンすることで、設定されたテンプレートのセキュリティを確保します。
- **部門間の連携の促進**：開発、運用、セキュリティの各チーム間の協力を促し、アプリケーションのライフサイクル全体を通じたセキュリティを統合することで、チーム間の連携を強化します。

今すぐ行動を起こす

目まぐるしく変化する今日のデジタル環境において、事後対応型のセキュリティモデルに依存しているということは、すでに遅れをとっていることを意味します。CNAPPで積極的なアプローチへの移行を今こそ検討すべきです。準備方法は以下の通りです。

- **脅威に先手を打つ**：脅威が顕在化する前にそれを予測し、軽減するためには、積極的なセキュリティ対策が不可欠です。CNAPPは、開発プロセスにセキュリティを組み込むことを可能にし、脆弱性に早期に対処できるようにします。
- **置き換えるのではなく、補完する**：CNAPPは既存のSIEMシステムを置き換えるのではなく、従来のツールが見逃していたセキュリティの穴を埋めるものです。SIEMは監視とログの記録に優れていますが、CNAPPはクラウドネイティブ環境に最適化された統合型のエンドツーエンドのセキュリティソリューションを提供します。この包括的なアプローチにより、クラウドインフラストラクチャのあらゆる部分が無防備な状態になることを防ぎます。
- **コストのかかるセキュリティ侵害を防ぐ**：クラウドの設定ミスは、セキュリティ侵害の主な原因です。このようなミスは、機密データを漏洩させ、重大な財務的、風評的損害をもたらす可能性があります。CNAPPは、クラウドインフラ全体にわたってセキュリティポリシーを継続的に監視し、適用することで、このような設定ミスが発生する前に防ぎます。

結論

多くの組織がクラウドファーストの企業環境を活用する中、CNAPPの導入を先延ばしにすることは、組織を重大なリスクにさらすことになります。従来型のセキュリティツールは、個別に存在し、事後対応型であるため、クラウドネイティブ環境のスピードと複雑性に対応しきれません。

CNAPPは、開発から運用に至るまで、アプリケーションのライフサイクル全体にわたってセキュリティを統合し、統一された積極的なアプローチを提供します。これにより、悪用される前に脆弱性を特定・対処することが可能になります。CNAPPの主なメリットは以下の通りです。

- **セキュリティ体制の強化**：CNAPPを導入することで、堅牢かつ予防的なセキュリティ体制を構築でき、クラウドネイティブ環境特有の課題に対処できるようになります。

- **運用の効率化**：CNAPPを統合することで、複数のセキュリティツールを管理する手間が軽減され、運用が合理化され、対応時間の短縮が実現します。

- **将来への備え**：クラウド環境が進化し続ける中、CNAPPのような包括的なセキュリティプラットフォームを導入することで、新たな脅威やコンプライアンス要件への対応が可能になります。

そして何より、対応を怠ることによる評判および財務上のリスクは非常に大きく、看過できません。設定ミス、データ漏洩、コンプライアンス違反は、コストと顧客の信頼の両面で大きな損害をもたらす可能性があります。CNAPPは、クラウドインフラを継続的に監視し、セキュリティポリシーを広範囲に適用することで、このような結果を防ぐことができます。

インシデントが発生してから動き出すのでは遅すぎます。今すぐCNAPPを導入し、クラウドインフラを保護し、データを守り、進化し続けるサイバーセキュリティの最前線に立ちましょう。

プロティビティのサイバーセキュリティコンサルティングについて

信頼と信用で未来を守る

イノベーションとデジタルトランスフォーメーションの加速、経済的期待、進化するサイバーセキュリティの脅威、人材不足、そして複雑化する規制環境、テクノロジーリーダーには、このような数多くの優先課題に効果的に対応し、管理することが求められています。

リスクを軽減しながら安全に成長するために、サイバーセキュリティ体制はビジネスの変化に適応し、対応する必要があります。テクノロジーが急速に進化し、デジタル化が加速する中、プロティビティのサイバーセキュリティ・プライバシーチームは、リスクをメリットに変え、組織のあらゆる層を保護し、安全に新たな機会に導きます。

私たちの戦略的で技術的な専門家は、お客様のサイバーセキュリティのニーズを十分に理解しています。私たちは、お客様のニーズに合わせたエンドツーエンドの次世代ソリューションの評価、開発、導入、運用を目指します。私たちは、お客様のデータを保護し、ビジネスとサイバーレジリエンスを最適化するための取り組みを提供しています。

その他の情報、事例、洞察については、プロティビティのサイバーセキュリティページをご覧ください。
プロティビティは法律事務所ではなく、本稿のいかなる内容も法的な目的のために使用されるべきものではありません。
法的助言が必要な場合は、社内または外部の法律顧問に相談してください。

protiviti®