DNP

クラウドワークロードセキュリティ
パート５ ： ３大クラウドプロバイダのセキュリティ機能比較

今回は、クラウドのセキュリティに関する５回シリーズの最終回です。パート１では、クラウド上のワークロードに対して、どのようにセキュリティ戦略を策定し、適切なコントロールを行うかをご紹介しました。バランスの取れたセキュリティ戦略は、実行時に違反を効率的に検知して対応しながら攻撃対象領域を減らしてくれることを見てきました。この戦略をうまく適用できるかどうかは、クラウドネイティブかサードパーティかにかかわらず、セキュリティコントロールとその実装を支援するソリューションにかかっています。

これらのツールをよりよく理解するために、前回までは、３大クラウド・サービス・プロバイダーである AWS、Azure、GCP が提供するさまざまなセキュリティ・ソリューションを紹介しました。

本シリーズの最終回では、ビッグ３が提供するコントロールを比較します。これにより、異なるクラウドにまたがるワークロードに対するクラウドセキュリティ戦略を定義する際に、参考となる情報をこの文書で得ることができます。

クラウドセキュリティコントロールとカテゴリ

クラウドのワークロードに適したセキュリティ戦略を導入するために、以下のようにいくつかのコントロールが用意されています。

- ネットワークセキュリティ
- 脆弱性管理
- ランタイムおよび Linux の脅威管理機能を備えたクラウドワークロード保護プラットフォーム（CWPP）
- クラウドセキュリティポスチャー管理（CSPM）
- SIEM 機能

- その他の脅威検知・監視機能

これらのセキュリティ対策の詳細については、パート 1 を参照してください。

これらのコントロールの大部分は、AWS、Azure、GCP のネイティブサービスを使って実装できます。ランタイムプロテクションや Linux の脅威検知など、サードパーティのソリューションで補強できる機能もいくつかあります。以下では、コントロールごとにそれぞれのクラウドプラットフォームの機能を比較します。

サービスの詳細については、このシリーズの AWS, Azure, GCP について特集したそれぞれのパートを参照ください。

ネットワーク

コントロール	(AWS)	(Azure)	(GCP)
ネットワークセグメンテーション	・仮想プライベートクラウド (VPC) ・セキュリティグループとネットワークアクセスコントロールリスト (ネットワークACL)	・仮想ネットワーク (VNet) ・ネットワークセキュリティグループ(NSG) ・アプリケーションセキュリティグループ（ASG) ・Azureファイアウォール	・仮想プライベートクラウド (VPC) ・ファイアウォールルール ・コンテナのネットワークポリシー
Webアプリケーションファイアウォール	・AWS WAF	・Azure WAF	・Google Cloud Armor
DDoS保護	・AWS Shield	・Azure DDoS protection	・Google Cloud Armor

表 1　ネットワークセキュリティコントロールの機能比較

クラウドセキュリティのポスチャ管理（CSPM）

コントロール	(AWS)	(Azure)	(GCP)
CSPM (VMやデータベースなどのクラウドワークロードにセキュリティ設定を行い、セキュリティベースラインに対するワークロードの状態を監視する)	・AWS Config ・Amazon Inspector ・AWS Security Hub ・AWS Audit Manager	・Azure Security Center	・Security Command Center

表 2　CSPM コントロールの機能比較

脆弱性管理

コントロール	(AWS)	(Azure)	(GCP)
パッチ管理	・AWS Systems Manager Patch Manager	・Azure Update Management	・OS patch management
ランタイムの脆弱性スキャンと管理	・Amazon Inspector	・Azure Security Center vulnerability assessment	・Cloud Security Scanner

表 3 脆弱性管理コントロールの機能比較

クラウドワークロード保護プラットフォーム（CWPP）

コントロール	(AWS)	(Azure)	(GCP)
ランタイム保護	・ネイティブのCWPPが利用できない場合は、Intezer Protectなどのサードパーティのツールを活用	・Microsoft Defender ・Linuxワークロードにセキュリティを追加し、Intezer Protectのようなサードパーティのソリューションによってインメモリの悪意のあるコードから保護。	・Intezer Protectなどのサードパーティ製ツールを活用し、ワークロード中心のセキュリティとランタイム保護を実現。
堅牢化されたVM	・ネイティブの堅牢化されたVMは利用できないため、CIS Hardened Imagesを使用	・ネイティブの堅牢化されたVMは利用できないため、CIS Hardened Imagesを使用	・Shielded VMs

表 4　CWPP コントロールの機能比較

コンテナセキュリティ

コントロール	(AWS)	(Azure)	(GCP)
イメージスキャニング	・ECR image scanning	・ACR container registry image scanning	・Container Analysis Service
コンテナ環境保護	・K8sの標準的なセキュリティ機能：IAM、セキュリティグループ、RBAC、ネットワークポリシー ・ランタイムスキャンと脆弱性管理のためのサードパーティ製ツールが必要	・ASC container environment protection	・Binary Authorizationによる信頼できるコンテナイメージの展開

表 5　コンテナセキュリティコントロールの機能比較

セキュリティ情報およびイベント管理（SIEM）

コントロール	（AWS）	(Azure)	（GCP）
SIEM (複数のソースからのデータを集約し、セキュリティインサイトを提供する)	・Security Hub が提供するSIEMのような機能はあるが、ネイティブのSIEMツールはない ・SIEM機能のためには、サードパーティのツールとの統合を推奨	・Azure Sentinel	・テレメトリデータを分析するためのChronicle Detectとの統合

表 6　SIEM コントロールの機能比較

その他の脅威検知機能

コントロール	（AWS）	(Azure)	（GCP）
クラウドアカウントレベルの脅威検知 (管理者権限での活動の監視とクラウドアカウントレベルでの脅威の的確な検知)	・Amazon GuardDuty ・Amazon Detective	・Azure Security Center threat protection	・Event Threat Detection

表 7　その他の脅威保護の機能比較

セキュリティログとモニタリング

コントロール	（AWS）	(Azure)	（GCP）
セキュリティログとモニタリング	・CloudWatch Logs ・CloudTrail ・VPC Flow Logs	・Azure Activity logs ・Azure AD logs ・NSG flow logs	・Cloud Audit Logs

表 8　セキュリティログとモニタリングの機能比較

まとめ

AWS、Azure、GCP のいずれも、重要なセキュリティコントロールを適用するためのツールやサービスを提供しています。これらのツールは、統合のしやすさ、サポート、管理のしやすさから推奨されています。

しかし、クラウドにおける脅威は進化しており、セキュリティを強化するためのより高度なツールが求められています。これは、Linux の脅威の検出、不正なコードの実行、インメモリの悪用などにおいて特に

重要です。Intezer Protect は、ネイティブのセキュリティツールやサービスと併用することで、信頼できるコードのみが実行されていることを 24 時間体制で保証することができます。

■原文

Intezer White Paper

Security Features of the Big 3 Cloud Providers

https://www.intezer.com/resources/whitepaper/security-features-of-the-big-3-comparison/

本稿は Intezer 社の許可を得て、同社のブログを翻訳したものです。翻訳を許諾いただいた Intezer 社に感謝します。

日本語版作成：2021 年 9 月

■免責事項

本稿は原文にできるだけ忠実に翻訳するよう努めていますが、完全性や正確性を保証するものではありません。翻訳監修主体は、本翻訳物に記載されている情報より生じる損失または損害に対して、いかなる人物あるいは団体にも責任を負うものではありません。原文の内容を理解する必要がある場合、上記の原文をお読み下さい。

翻訳監修主体：大日本印刷株式会社　AB センターDX 事業開発本部サイバーセキュリティ事業推進ユニット

■関連コンテンツ

クラウドワークロードセキュリティ

パート 1：知っておくべきこと（https://www.dnp.co.jp/cka/column/column-vol06.html）

パート 2：AWS のセキュリティ機能（https://www.dnp.co.jp/cka/column/column-vol07.html）

パート 3 ：Azure のセキュリティ機能（https:/www.dnp.co.jp/cka/column/column-vol09.html）

パート 4 ：GCP のセキュリティ機能（https:/www.dnp.co.jp/cka/column/column-vol11.html）

パート 5：3 大クラウドプロバイダのセキュリティ機能 <本稿>