

総務省 御中

IPネットワーク設備委員会 作業班 第3回 ヒアリング項目へのご回答

アマゾン ウェブ サービス ジャパン合同会社

2026年4月30日

1. 電気通信事業者への提供状況、 今後の方針

電気通信設備における AWS の活用事例

O2 Telefónica（独）

NTT DOCOMO

[Back to Press Releases Telefónica Germany](#)

05.03.2025

O₂ Telefónica selects Amazon Web Services for its cloud-native IMS voice and 5G core networks



O₂ Telefónica brings 5G cloud core to own data center with Nokia and AWS Outposts

03.03.2026



The core network usually consists of several data centers in which the data traffic is processed (Credits: Gettyimages)

Telecommunications provider O₂ Telefónica today announced a strategic shift in the operation of its 5G Core network, becoming the first telecommunications operator worldwide to move production-scale network functions to AWS Outposts deployed in its own data center. O₂ Telefónica is using technology from European network equipment supplier Nokia to run its 5G core network on AWS infrastructure. As data traffic, digital services and real-time applications continue to grow, O₂ Telefónica is modernizing how it operates 5G core networks. By moving key functions into a cloud-based architecture hosted in its own data center, the company is strengthening network stability, speeding up innovation and ensuring consistent performance for customers.

At Mobile World Congress, O₂ Telefonica in Germany announced that they have selected Amazon Web Services, Inc. (AWS), an Amazon.com company (NASDAQ: AMZN) as cloud provider for network workloads. As part of the multi-year agreement, following the successful deployment of its 5G SA Core on AWS in July last year, O₂ Telefónica will expand the current 5G core implementation on AWS, deploying 5G core data plane in its data centers through the new AWS Outposts racks for high throughput, network-intensive workloads. As part of the agreement O₂ Telefónica will also deploy IMS voice in the AWS-cloud on AWS Graviton processors starting from this year.

O₂ Telefónica will benefit from AWS Cloud Continuum to extend AWS cloud services to the furthest edge of its 5G network, leveraging same platform, APIs, and tools, to achieve cost efficient capacity scaling to meet the growing throughput demands on one of the most will enable superior end-customer experiences, faster and agile network automation, easier integration and operations leveraging cloud native and IMS voice domains. The German telecommunications provider will include Amazon CloudWatch, Amazon Managed Service for Prometheus simplify 5G network operations with advanced analytics of network metrics Amazon Athena and Amazon SageMaker.

March 02, 2026

NTT ドコモ、AWS 上で 5G コアネットワークの商用運用を開始

AI エージェント活用でネットワーク構築期間を約 80%、障害対応時間を約 50% 短縮し、通信インフラの革新を加速

アマゾン ウェブ サービス ジャパン合同会社（以下、AWS ジャパン）は、株式会社 NTT ドコモ（以下、ドコモ）が通信事業者としてアジア太平洋地域で初めて、AWS のクラウドサービスと同社の仮想化基盤（オンプレミス）を活用したハイブリッド環境上で 5G コアネットワーク（以下、5GC）の商用サービスを開始したことを発表しました。AWS は 2022 年から、ドコモ、および、5GC ソフトウェアを提供する日本電気株式会社（以下、NEC）と技術検証を進め、強靱性と俊敏性、柔軟性に優れたキャリアグレードの通信インフラストラクチャの構築に向けて取り組んできました。さらに今回の商用展開では、AI エージェントを活用して 5GC の設計・構築を自動化し、構築期間を約 80% 短縮しています。3 社が連携した通信インフラの革新により、安定した通信サービスの提供、新サービスの迅速な市場投入を可能とする基盤を確立することで、顧客体験の継続的な向上を実現します。

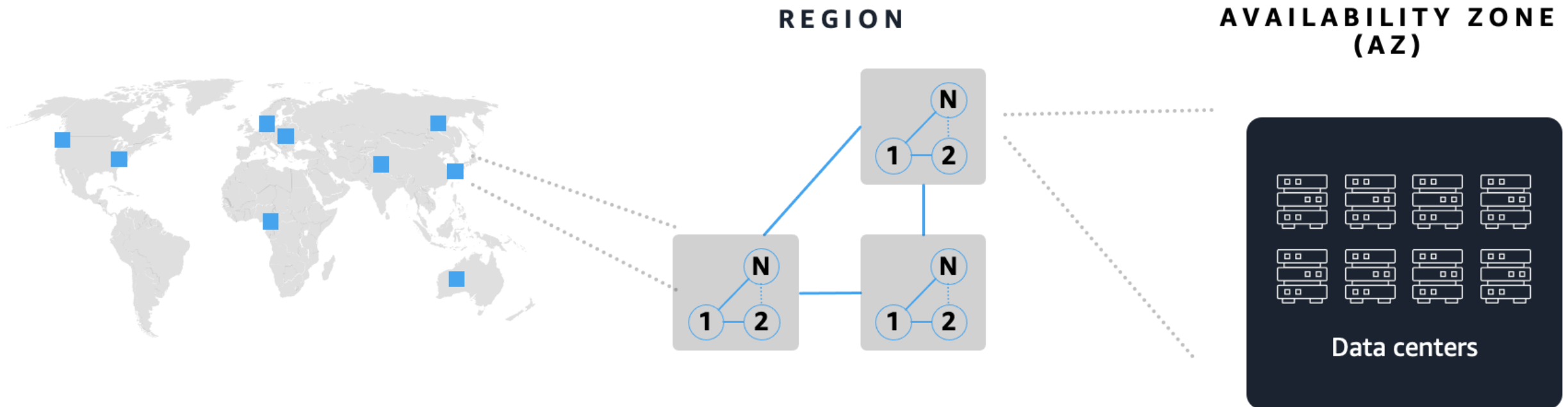
9,100 万*契約者へのサービス提供を支える次世代インフラ

ドコモは今回の商用開始を皮切りに、順次同社 5G サービスを AWS とのハイブリッド構成に移行していきます。信頼性と経済性に優れた同社の仮想化基盤を活かしながら、AWS の包括的な AI 機能および実績のあるクラウドインフラストラクチャを組み合わせることで、ネットワークの強靱性をさらに高めながら、俊敏性と柔軟性を実現します。また AWS 上では、電力効率に優れた独自設計のチップセットである [AWS Graviton プロセッサ](#) を活用して 5GC を構築することで環境負荷を低減します。ドコモによる今回の AWS を活用した 5GC の商用展開は、アジア太平洋地域における重要なマイルストーンです。

技術基準への適合性

- 予備機器等（事業用電気通信設備規則第4条）

- AWS リージョンは、1つの地理的エリアにある最低3つの、物理的に分離され、独立した電源・ネットワーク・冷却設備を持つ、アベイラビリティゾーン（AZ）と呼ばれる論理的データセンターのグループによって構成されています。通信事業者はリージョンもしくはアベイラビリティゾーンを横断して自身で予備機器等を備えることができる他、AWS のマネージドサービスにおいては予め AWS がリージョンや AZ をまたがって構成した冗長構成を利用することもできます。



技術基準への適合性

- 電源設備（同規則第10条）、停電対策（同規則第11条）
 - AWSのデータセンターの電力システムは、完全に冗長性をもち、1日24時間・週7日、運用に影響を与えることなくメンテナンス可能な設計がなされています。データセンターは、施設全体へのバックアップ電力を供給する発電機を備えている他、施設内の重要かつ不可欠な箇所における電力障害に際しては、無停電電源装置（UPS）がバックアップ電力を供給します。なお、発電機、UPSともに複数系統のN+1以上の冗長構成であり、単一障害点がない設計となっております。



サービスの品質保証

Region-Level SLA

For Amazon EC2 with all running instances deployed concurrently across two or more AZs in the same region (or at least two regions if there is only one AZ in a given region), AWS will use commercially reasonable efforts to make Amazon EC2 available for each AWS region with a Monthly Uptime Percentage of at least 99.99%, in each case during any monthly billing cycle (the "Region-Level SLA"). In the event Amazon EC2 does not meet the Region-Level SLA, you will be eligible to receive a Service Credit as described below.

Monthly Uptime Percentage	Service Credit Percentage
Less than 99.99% but equal to or greater than 99.0%	10%
Less than 99.0% but equal to or greater than 95.0%	30%
Less than 95.0%	100%

(例) Amazon EC2 のリージョンレベル SLA

AWS は一般に利用可能なすべての有料サービスについて**サービスレベル契約 (SLA)** を提供することを約束します。

たとえば、コンピュートの**Amazon EC2** ではリージョンレベルのSLAを**99.99%** と定義しています。同様にデータベースの**Amazon Aurora**のマルチAZ構成では**99.99%**、分散データベースの**Amazon Aurora DSQL**では**99.999%**です。サービスクレジット率はいずれも10%です。

設計の品質保証

AWS Well-Architected は、クラウドアーキテクトがさまざまなアプリケーションやワークロード向けに安全性、高い性能、障害耐性、効率性を備えたインフラストラクチャを構築する際に役立ちます。**6つの柱**に基づいて、お客様とパートナーがアーキテクチャを評価し、スケーラブルな設計を実装するための一貫したアプローチを提供しています。

優れた運用効率

システムの実行とモニタリング、およびプロセスと手順の継続的な改善に焦点を当てています。主なトピックには、変更の自動化、イベントへの対応、日常業務を管理するための標準化などが含まれます。

セキュリティ

情報とシステムの保護に焦点を当てています。主なトピックには、データの機密性と完全性、ユーザー許可の管理、セキュリティイベントを検出するためのコントロールの確立が含まれます。

信頼性

期待どおりの機能を実行するワークロードと、要求に応えられなかった場合に迅速に回復する方法に焦点を当てています。主なトピックには、分散システムの設計、復旧計画、および変化する要件への処理方法が含まれます。

パフォーマンス効率

IT およびコンピューティングリソースの構造化および合理化された割り当てに重点を置いています。主なトピックには、ワークロードの要件に応じて最適化されたリソースタイプやサイズの選択、パフォーマンスのモニタリング、ビジネスニーズの進化に応じて効率を維持することが含まれます。

コスト最適化

不要なコストの回避に重点を置いています。主なトピックには、時間の経過による支出の把握と資金配分の管理、適切なリソースの種類と量の選択、および過剰な支出をせずにビジネスのニーズを満たすためのスケーリングが含まれます。

持続可能性

実行中のクラウドワークロードによる環境への影響を最小限に抑えることに重点を置いています。主なトピックには、持続可能性の責任共有モデル、影響についての把握、および必要なリソースを最小化してダウンストリームの影響を減らすための使用率の最大化が含まれます。

情報保全への対応

AWS 責任共有モデル

お客様

Security “IN” the Cloud
クラウド内のセキュリティ

お客様のデータ

プラットフォーム、アプリケーション、IDとアクセス管理

オペレーティングシステム、ネットワーク、ファイアウォール構成

クライアント側のデータ暗号化
とデータ整合性認証

サーバー側の暗号化
(ファイルシステムやデータ)

ネットワークトラフィック保護
(暗号化、整合性、アイデンティティ)

AWS

Security “OF” the Cloud
クラウドのセキュリティ

ソフトウェア

コンピューート

ストレージ

データベース

ネットワーキング

ハードウェア / グローバルインフラストラクチャー

リージョン

アベイラビリティ
ゾーン

エッジロケーション

情報保全に関する脅威

AWS 責任共有モデル

お客様

Security "IN" the Cloud
クラウド内のセキュリティ

AWS

Security "OF" the Cloud
クラウドのセキュリティ

サイバー攻撃に
対する防御

クラウド
オペレーター
からの保護

サイバー攻撃に対する防御

AWS 脅威インテリジェンス



MadPot

世界規模の攻撃情報分析

数万台のハニーポッドを設置

攻撃者を偽装されたデジタルターゲットに誘導、攻撃手法を収集・分析



Sonaris

潜在的な悪性ネットワーク トラフィックを分析し防御

AWS のインフラとサービスを狙う不審な行動を検出し遮断

EC2 上の脆弱性のスキャンを 2.7 兆回、公開 S3 バケットのスキャンを 270 億回ブロック



Mithra

悪性ドメイン分析システム

35 億のノードと 480 億のエッジを持つニューラルネットワークグラフモデル

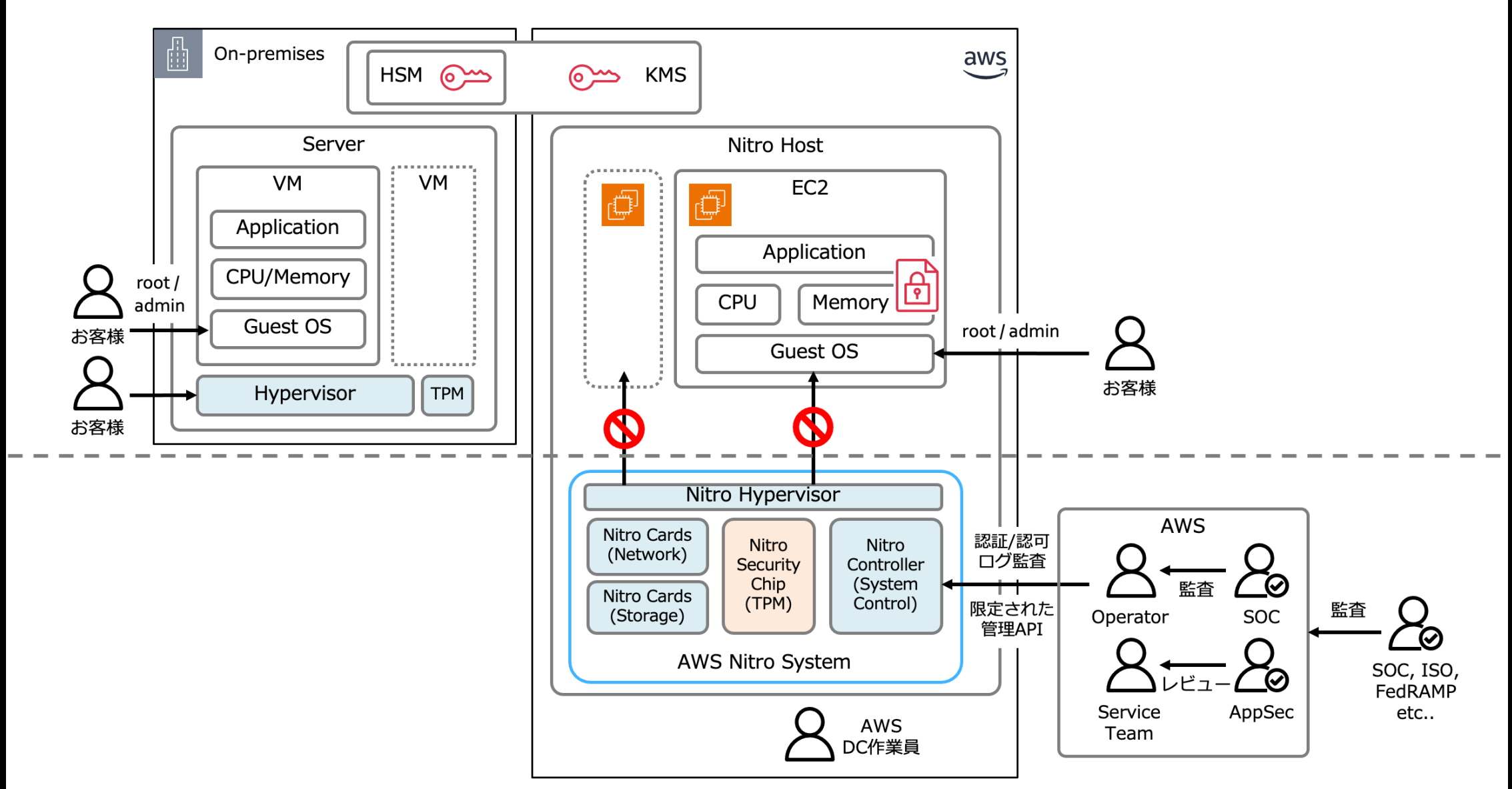
毎日 1 兆を超えるドメインリクエストを観察し平均 12.4 万の悪性ドメイン検出

クラウドオペレーターからの保護

コンフィデンシャルコンピューティング (Confidential Computing)

1. 基盤ホストにログインする仕組みはない
2. 管理用APIは基盤ホスト上の顧客コンテンツにアクセスできない
3. 管理用APIへのアクセスには常に認証と認可が必要となる
4. 管理用APIへのアクセスは常にログに記録される
5. ホストはテスト済み・署名済みのソフトウェアのみを実行できる
6. ホストに直接コードを配置することはできない
7. 保存された顧客コンテンツにアクセスする仕組みはない
8. 暗号化された通信データにアクセスする仕組みはない
9. 様々なEC2インスタンスでメモリ暗号化機能を提供

AWS Nitro System による管理者オペレーションの統制



AWS Nitro System





2015 年の半導体開発企業の買収を契機に**シリコン開発を内製化**

ストレージ、ネットワーク、セキュリティなどの性能を高める
カード／チップを開発



AWS Nitro System

パフォーマンス

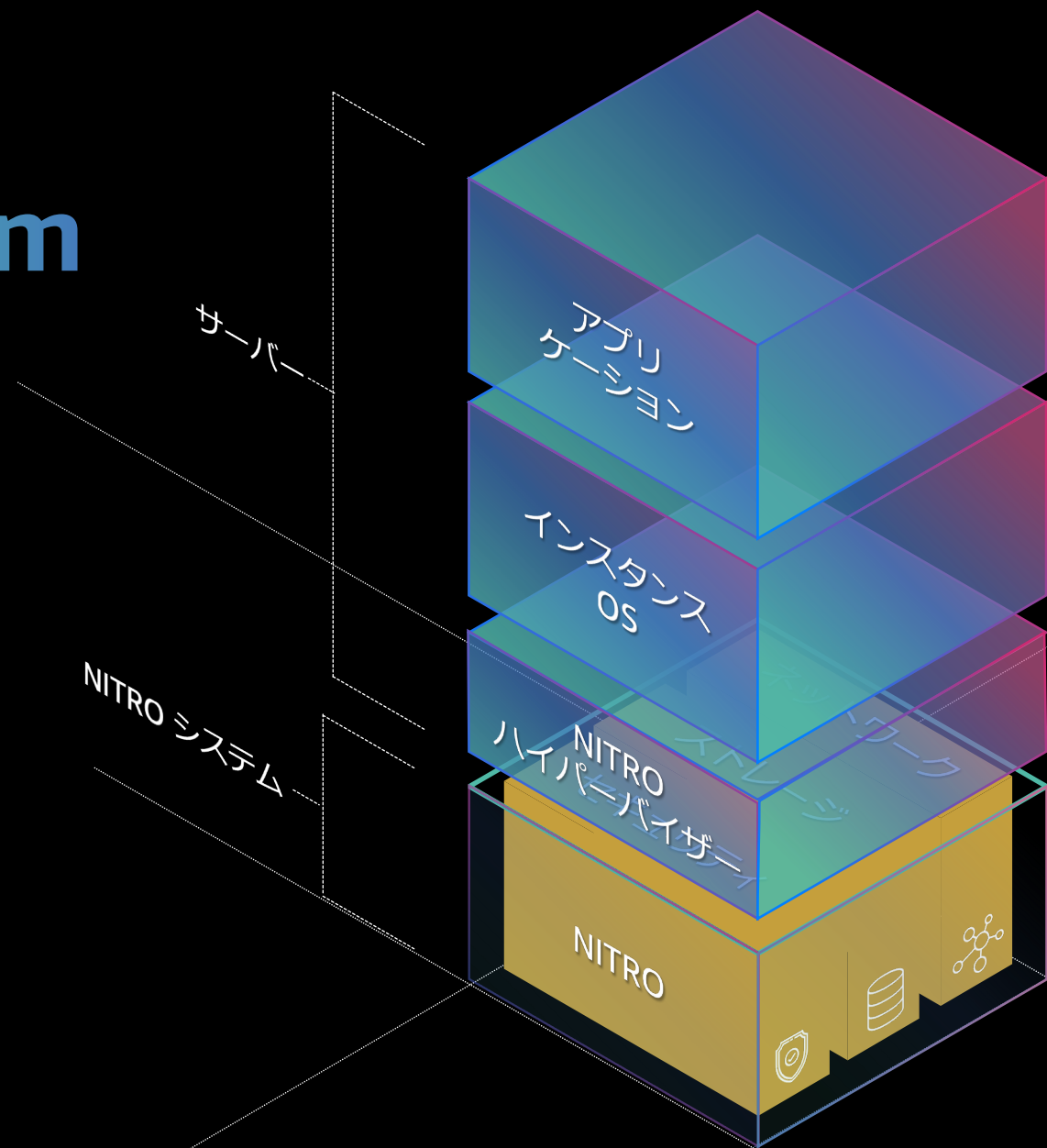
ネットワークおよびストレージ性能の
さらなる向上

アジリティ

あらゆるサーバーを完全な EC2
インスタンスとして活用可能

セキュリティ

ハードウェアによる分離の強制



AWS Nitro System

パフォーマンス

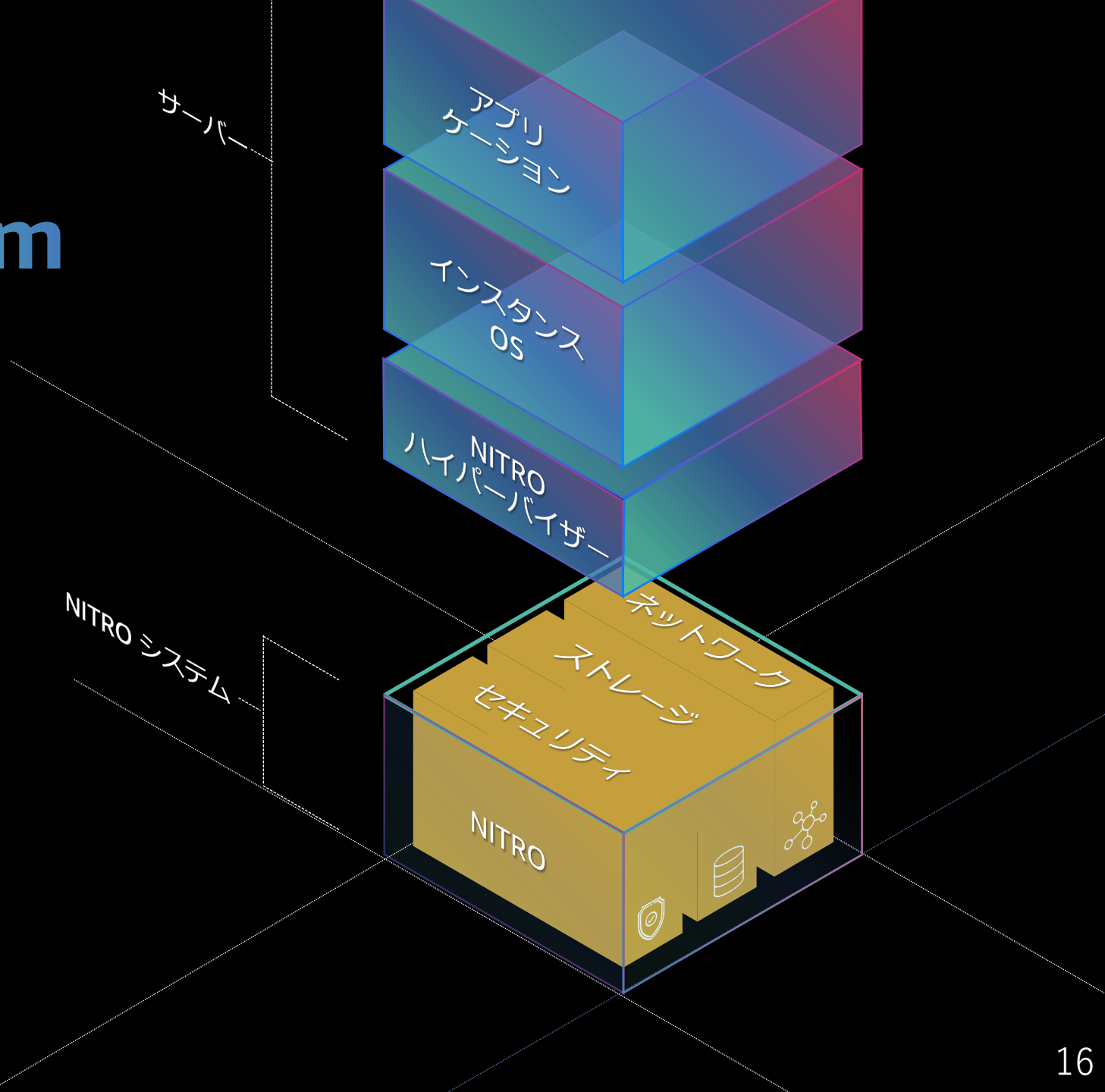
ネットワークおよびストレージ性能の
さらなる向上

アジリティ

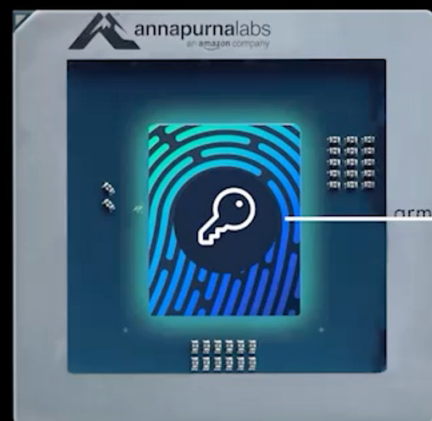
あらゆるサーバーを完全な EC2
インスタンスとして活用可能

セキュリティ

ハードウェアによる分離の強制



AWS Nitro チップ



公開鍵

秘密鍵を基に
公開鍵・秘密鍵ペアを生成される。
公開鍵は安全な製造記録の一部となる。

秘密鍵

製造時に固有の鍵が生成・保存され、
「指紋」として機能。
鍵はチップの外には出ない。

Nitro が信頼の基点



- 認証完了
- ファームウェアのバージョン
- プロセッサの識別情報
- チップの製造品質

2. 障害発生時の対応について

サービス稼働状況に関する情報提供

稼働状況・セキュリティ

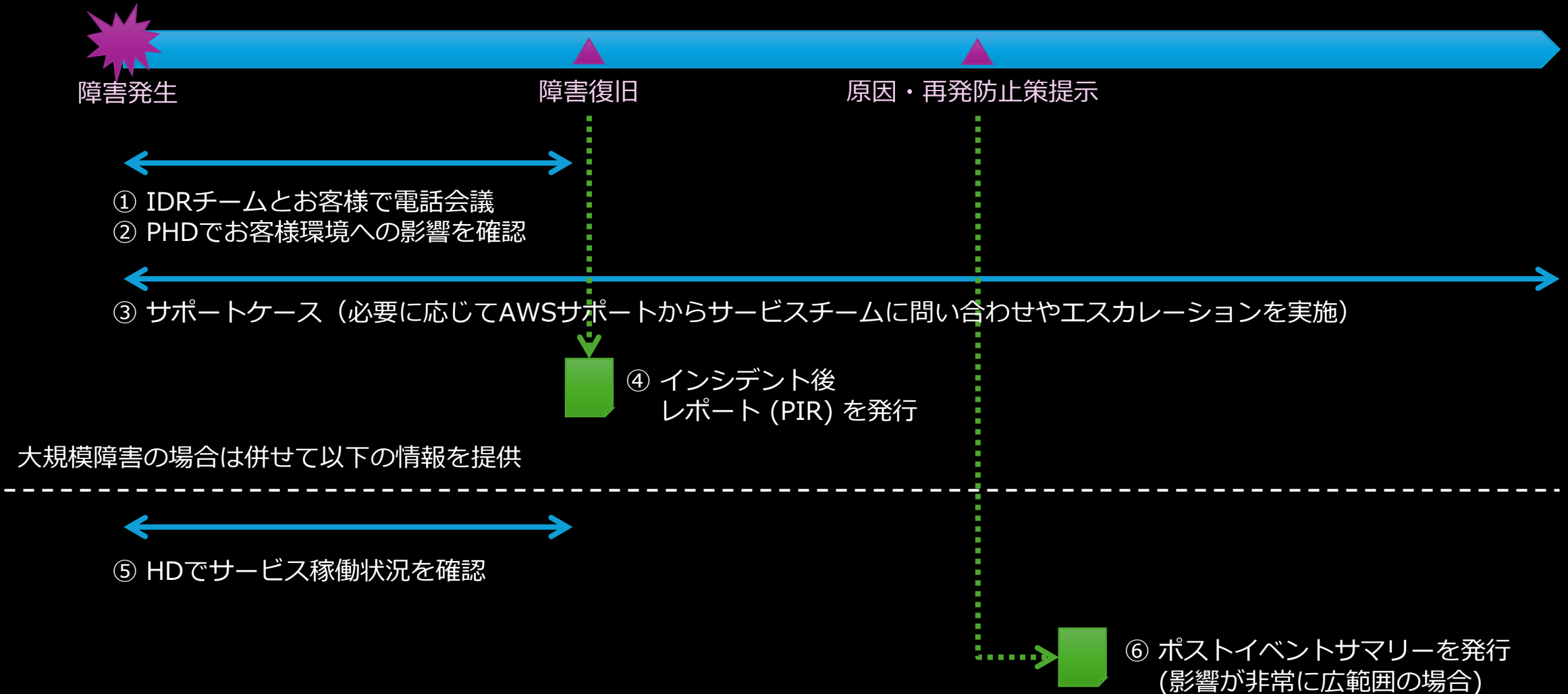
ヘルスダッシュボード (HD: Health Dashboard)	- AWSサービスの最新の稼働状況と過去12ヶ月間の履歴を公開 - 障害発生時はリージョン、サービス名、重要度、タイムライン、影響を受けたサービスをAWSの判断で公開
パーソナルヘルスダッシュボード (PHD: Personal Health Dashboard)	お客様の環境に影響を及ぼす可能性のあるAWSイベントのアラートやガイダンスを提供
セキュリティ速報 (Security Bulletins)	報告されたすべてのセキュリティ脆弱性から、AWSのサービス、ソフトウェア、製品に影響を及ぼすものを公開

障害対応

サポートケース (Case: Support Case)	- お客様からの問い合わせに基づき、サービスに関連する技術的な問題について対応 - 初回応答時間はSeverityにより異なる - ケースの返答時間は解析状況によるが、次の状況報告のタイミングを連絡
インシデント後レポート (PIR: Post Incident Report)	- 重要ワークロードに対するプロアクティブなインシデント対応 (IDR: Incident Detection Response) に付随 - お客様からのリクエストに基づき復旧対応レポートを提供 - 問題、影響、関与したチーム、取られた回避策/アクションが含まれる - Unified Operations（最上位サポート）の契約が必要
ポストイベントサマリー (PES: Post Event Summary)	- ある問題がお客様に広範かつ重大な影響を及ぼした場合に、問題の解決後にAWSの判断で公開する - コントロールプレーンのAPI呼び出しがかなりの割合で失敗する、サービスの基盤やリソースもしくはAPIにかなりの割合で影響する、全面的な電源障害や重大なネットワーク障害に至るなど - 問題の影響範囲、問題の原因となった要因、特定されたリスクに対処するために取られた措置が記載される 2025/10/20の大規模障害の際は、英語バージョンを10/23、日本語バージョンを10/29に公開

障害発生時におけるAWSからの情報提示の流れ

Unified Operations（最上位サポート）の場合



レポート出力の例

AWS Health Dashboard

自動更新

1分未満前に更新

アカウントの状態を表示

AWS アカウントまたは組織に影響するイベントのパーソナライズされたビューを取得します。

アカウントの状態を開く

サービスの状態

すべての AWS サービスの現在および過去のステータスを表示します。

未解決の問題と最近の問題 (0)

ステータス履歴

最近の問題はありません

1分未満前に更新

ステータス履歴

サービス一覧 イベント一覧

次の表は、過去 12 か月間の AWS のサービスの中断の実行ログを示しています。そのサービスのステータスの更新を表示するには、ステータスアイコンを選択します。すべての日付と時刻は、現地時間 (ブラウザのタイムゾーン) でレポートされます。タイムゾーンを更新するには、「タイムゾーン設定」を参照してください。

AWS のサービスまたはリージョンを検索

ロケール
北米

<< 2026/01/21

1 2 3 4 5 6 7 ... 26 >>

YYYY/MM/DD 形式を使用してください。

サービス	RSS	本日	20 1月	19 1月	18 1月	17 1月	16 1月	15 1月
Amazon API Gateway (Calgary)	📡	🟢	🟢	🟢	🟢	🟢	🟢	🟢
Amazon API Gateway (Canada-Central)	📡	🟢	🟢	🟢	🟢	🟢	🟢	🟢
Amazon API Gateway (Mexico-Central)	📡	🟢	🟢	🟢	🟢	🟢	🟢	🟢
Amazon API Gateway (N. California)	📡	🟢	🟢	🟢	🟢	🟢	🟢	🟢
Amazon API Gateway (N. Virginia)	📡	🟢	🟢	🟢	🟢	🟢	🟢	🟢
Amazon API Gateway (Ohio)	📡	🟢	🟢	🟢	🟢	🟢	🟢	🟢
Amazon API Gateway (Oregon)	📡	🟢	🟢	🟢	🟢	🟢	🟢	🟢
Amazon AppFlow (Canada-Central)	📡	🟢	🟢	🟢	🟢	🟢	🟢	🟢
Amazon AppFlow (N. California)	📡	🟢	🟢	🟢	🟢	🟢	🟢	🟢
Amazon AppFlow (N. Virginia)	📡	🟢	🟢	🟢	🟢	🟢	🟢	🟢
Amazon AppFlow (Ohio)	📡	🟢	🟢	🟢	🟢	🟢	🟢	🟢
Amazon AppFlow (Oregon)	📡	🟢	🟢	🟢	🟢	🟢	🟢	🟢
Amazon Athena (Calgary)	📡	🟢	🟢	🟢	🟢	🟢	🟢	🟢
Amazon Athena (Canada-Central)	📡	🟢	🟢	🟢	🟢	🟢	🟢	🟢
Amazon Athena (Mexico-Central)	📡	🟢	🟢	🟢	🟢	🟢	🟢	🟢

Health Dashboard (HD)

AWS Health Dashboard

自動更新

1分未満前に更新

アカウントの状態

Stay informed of important events affecting your AWS resources.

Amazon EventBridge ルール

サービスおよびリソースに影響する可能性のあるイベントの通知を取得します。

設定 詳細はこちら

未解決の問題と最近の問題 (0)

スケジュールされた変更 (0)

その他の通知 (0)

イ

最近の問題はありません

1分未満前に更新

未解決の問題と最近の問題 (0)

AWS インフラストラクチャに影響する可能性のあるイベントを表示します。過去 24 時間以内の 0 個の問題点が解決されました。

検索および追加フィルター

1

🔧

イベント

リージョン/ゾーン
詳細情報

開始時刻

最終更新日時

影響を受けるリソース

イベントはありません。

Personal Health Dashboard (PHD)

レポート出力の例

Post ** Incident ** Report ** Template
Post Incident Report - 0000000123
Customer: Example Customer
AWS Support case ID(s): 0000000000
Customer internal case ID (if provided): 1234567890
Incident start: 2023-02-04T03:25:00 UTC
Incident resolved: 2023-02-04T04:27:00 UTC
Total Incident time: 1:02:00 s
Source Alarm ARN: arn:aws:cloudwatch:us-east-1:000000000000:alarm:alarm-

Problem Statement:

Outlines impact to end users and operational infrastructure impact.
Starting at 2023-02-04T03:25:00 UTC, the customer experienced a large s

Incident Summary:

Summary of the incident in chronological order and steps taken by AWS Ir
At 2023-02-04T03:25:00 UTC, the workload impairments alarm triggered c
At 2023-02-04T03:28:00 UTC, ** per the runbook, the alarm had not recc
At 2023-02-04T03:32:00 UTC, ** the customer's SRE team, and Support Er
At 2023-02-04T03:45:00 UTC, the Cloud Support Engineer discovered a su
At 2023-02-04T03:56:00 UTC, the customer instituted back off and retry
At 2023-02-04T04:05:00 UTC, ALB support team initiates scaling activit
By 2023-02-04T04:15:00 UTC, scaling activities complete and metrics/alc
At 2023-02-04T04:27:00 UTC, per the runbook the call was spun down, af

Mitigation:

Describes what was done to mitigate the issue. NOTE: this is not a Root
Back-off and retries yielded mild recovery. Full mitigation happened c

Follow up action items (if any):

Action items to be reviewed with your Technical Account Manager (TAM), i
Review alarm thresholds to engage AWS Incident Detection and Response cl
Work with AWS Support and TAM team to ensure newly created ALBs are pre-

東京リージョン (AP-NORTHEAST-1) で発生した Amazon EC2 と Amazon EBS の事象概要

2019年8月28日(日本時間)更新:

最初の事象概要で言及した通り、今回のイベントは、東京リージョンの1つのアベイラビリティゾーン(AZ)の一部に影響を与えました。この影響は当該 AZ の Amazon EC2 および Amazon EBS のリソースに対するものですが、基盤としている EC2 インスタンスが影響を受けた場合には、当該 AZ の他のサービス(RDS、Redshift、ElastiCache および Workspaces 等)にも影響がありました。お客様と今回のイベントの調査をさらに進めたと、個別のケースのいくつかで、複数のアベイラビリティゾーンで稼働していたお客様のアプリケーションにも、予期せぬ影響(例えば、Application Load Balancer を AWS Web Application Firewall やスティーキーセッションと組み合わせてご利用しているお客様の一部で、想定されるより高い割合でリクエストが Internal Server Error を返す)があったことを AWS では確認しております。AWS では、個別の問題についての詳細な情報を、影響を受けたお客様に直接、共有を行う予定です。

2019年8月28日(日本時間)更新:

最初の事象概要で言及した通り、今回のイベントは、東京リージョンの1つのアベイラビリティゾーン(AZ)の一部に影響を与えました。この影響は当該 AZ の Amazon EC2 および Amazon EBS のリソースに対するものですが、基盤としている EC2 インスタンスが影響を受けた場合には、当該 AZ の他のサービス(RDS、Redshift、ElastiCache および Workspaces 等)にも影響がありました。お客様と今回のイベントの調査をさらに進めたと、個別のケースのいくつかで、複数のアベイラビリティゾーンで稼働していたお客様のアプリケーションにも、予期せぬ影響(例えば、Application Load Balancer を AWS Web Application Firewall やスティーキーセッションと組み合わせてご利用しているお客様の一部で、想定されるより高い割合でリクエストが Internal Server Error を返す)があったことを AWS では確認しております。AWS では、個別の問題についての詳細な情報を、影響を受けたお客様に直接、共有を行う予定です。

2019年8月25日(日本時間)初版:

日本時間 2019年8月23日 12:36 より、東京リージョン (AP-NORTHEAST-1) の単一のアベイラビリティゾーンで、オーバーヒートにより一定の割合の EC2 サーバの停止が発生しました。この結果、当該アベイラビリティゾーンの EC2 インスタンスへの影響及び EBS ボリュームのパフォーマンスの劣化が発生しました。このオーバーヒートは、影響を受けたアベイラビリティゾーン中の一部の冗長化された空調設備の管理システム障害が原因です。日本時間 15:21 に冷却装置は復旧し、室温が通常状態に戻り始めました。室温が通常状態に戻ったことで、影響を受けたインスタンスの電源が回復しました。日本時間 18:30 までに影響を受けた EC2 インスタンスと EBS ボリュームの大部分は回復しました。少数の EC2 インスタンスと EBS ボリュームは、電源の喪失と過大な熱量の影響を受けたハードウェアホスト上で動作していました。これらのインスタンスとボリュームの復旧には時間がかかり、一部につきましては基盤のハードウェアの障害によりリタイアが必要でした。

EC2 インスタンスと EBS ボリュームへの影響に加えて、EC2 RunInstances API にも影響が発生しました。日本時間 2019年8月23日 15:21 に、影響の発生したアベイラビリティゾーンでの EC2 インスタンスの起動、および冪等性トークン (複数のインスタンスを起動させる危険なく、インスタンスの起動をリトライする機能) を使用して RunInstances API を東京リージョンで実行した場合に、エラー率の上昇が発生しました。その他の EC2 API や冪等性トークンを使用しない EC2 インスタンスの起動は正常に動作しておりました。この問題は、冪等性トークンを使用する Auto Scaling グループからのインスタンスの新規起動も阻害しました。日本時間 14:51 に、エンジニアは、冪等性トークンと Auto Scaling グループの問題を解決しました。影響の発生したアベイラビリティゾーンでの、新しい EC2 インスタンスの起動についてのエラー率向上は、EC2 コントロールプレーンサブシステムのリストアが完了した日本時間 16:05 まで継続しました。影響の発生した EBS ボリュームのスナップショットの作成も、この期間にエラー率の上昇が発生しました。

今回の事象はデータセンターで使用されるいくつかの冷却システムの制御と最適化に使用されるデータセンター制御システムの障害によって引き起こされました。制御システムは、高可用性を実現するために複数のホストで実行されます。この制御システムには、ファン、冷却装置、温度センサーなどのサードパーティ製デバイスとの通信を可能にするサードパーティ製のコードが含まれていて、直接または組み込みプログラマブルロジックコントローラ (PLC) を介して通信し、実際のデバイスと通信します。今回の事象発生の直前に、データセンター制御システムは、制御ホスト群から制御ホストの1つを外す処理を行っていました。このようなフェイルオーバーの間、新しい制御ホストがデータセンターの最新状況を保持する為に、制御システムは、他の制御システムおよび制御するデータセンター機器 (データセンター全体の冷却装置および温度センサーなど) と情報を交換する必要があります。サードパーティ製の制御システムにおけるロジックのバグにより、この情報交換が制御システムとデータセンターのデバイス間で過度に発生し、最終的には制御システムが応答しなくなりました。AWS のデータセンターは、データセンターの制御システムに障害が発生した場合、制御システムの機能が回復するまで冷却システムが最大冷却モードになるよう設計されています。これはデータセンターのほとんどで正常に機能していましたが、データセンターのごく一部で冷却システムがこの安全な冷却構成に正しく移行できず停止しました。

インシデント後レポート (PIR)

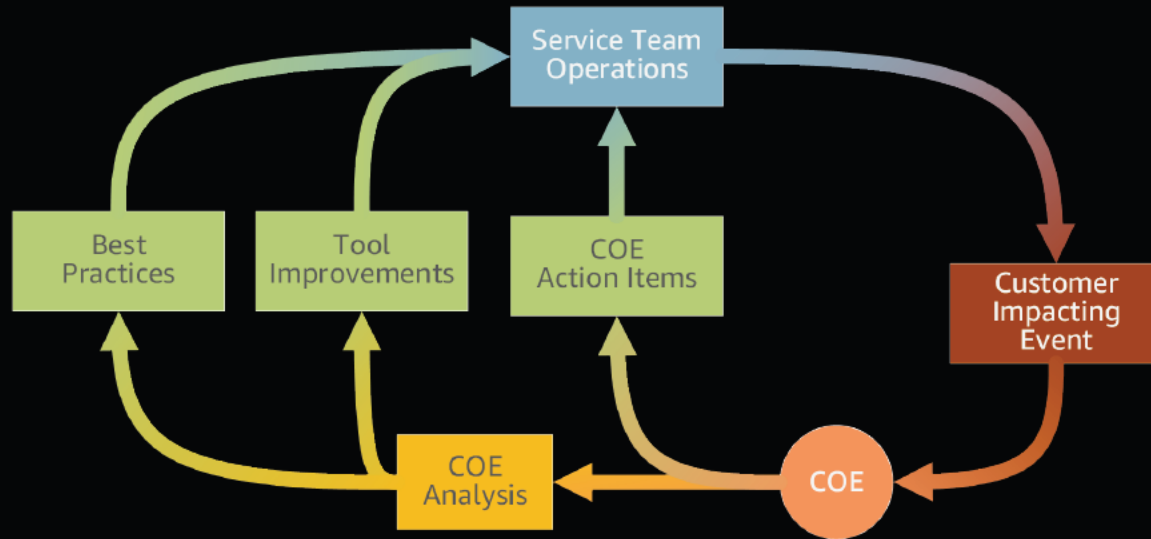
ポストイベントサマリー (PES)

ポストイベントサマリー (PES) の例

2019年8月 EC2/EBS障害

関連項目	記載例
発生場所	東京リージョンの一つのAZ、一部データセンターなど、発生場所を記載
事故の全体概要	EC2/EBS リソースの立ち上げ/操作不能、Snapshot失敗、Auto Scalingの機能不全など、クラウド機能単位での影響を具体的に記載
原因となった設備の概要	冷却設備、制御装置、PLC、電力制御との関係などを記載
発生状況 (影響範囲・利用者数)	EC2インスタンス、EBS ボリューム、EC2 RunInstances APIへの影響を記載 (電気通信役務としての影響範囲や利用者数は通信事業者にて記載)
措置模様 (対応の時系列)	発生から復旧までの経過を詳細に記載
発生原因 (管理工程ごとの分析含む)	第三者コードのロジック不具合、PLCが応答を失い冷却装置が停止、フェイルオーバー機能が働かずなど、原因を記載
再発防止策	応急対処（手動リブート、設備切り離し）、恒久対策（フェイルモード廃止、トレーニング強化）など、再発防止策を記載

再発防止に向けた取り組み



Correction of Error (CoE) と呼ばれる障害分析のプロセスで、障害の概要、それを観測したメトリクス、影響や時系列のイベント、障害からの学びや改善に向けたアクションといった項目を徹底的に振り返ります。

AWSマネジメントは、少なくとも月次ベースで、AWSの運用メトリクスおよびCOEをレビューし、AWSサービス全体の可用性を向上させ、AWS環境へのリスクを軽減しながら改善領域を特定しています。

チームを横断する形でオペレーションのナレッジを共有するWeekly Operations Reviewsにおいても、大規模や教訓が得られるCOEを選んで共有しています。このミーティングでは、ルーレットで選ばれたサービスチームのダッシュボードを使って、サービスの状態やオペレーションの健全性を説明し、他のチームから質問や指摘を受ける、というユニークな取り組みが行われています。これにより、すべてのチームがダッシュボードをメンテナンスし、状態を定期的にチェックするようになります。



3. 要望事項など

制度整備を行う場合の要望

1. 技術基準適合に関する自己確認届出内容の標準化

- ・ 事業要電気通信設備をクラウドサービスのような他者設備に構築する場合に、現状では電気通信事業者が個別にクラウドサービス事業者にお問い合わせを行い、自己確認届出内容を確認・記述しています。
- ・ クラウドサービス事業者の立場からは、各電気通信事業者が設備を構築する都度、個別の対応が求められます。加えて、問い合わせごとに確認事項が異なるため、関連部門における業務負荷の増大に苦慮しているのが実情です。こうした状況は、クラウドサービス事業者に限ったものではなく、問い合わせを行う各電気通信事業者においても、確認項目の策定や回答内容の精査等に相応の負担が生じているものと推察いたします。
- ・ たとえば、今回ご説明した予備機器等（事業用電気通信設備規則第 4 条）、電源設備（同規則第 10 条）、停電対策（同規則第 11 条）のような共通的な項目について、**ISMAPのようなガイドラインを通じて要求水準を明確化してクラウドサービス事業者を認定**することで、電気通信事業者が個別に確認することなくクラウドサービスを活用できるよう、制度整備をいただきたく存じます。

2. 通信の秘密とクラウド利用についての考え方の明確化

- ・ 総務省の「クラウドネイティブな情報通信ネットワークを前提とする」との方針に関わらず、電気通信事業者によっては、通信の秘密の関係からクラウドサービスのような他者設備でデータを扱うことについて、通信の秘密の観点から躊躇したり不安を感じるなどの課題が存在し、活用の阻害要因となっています。
- ・ 今回ご説明した **AWS Nitro System** のような**コンフィデンシャルコンピューティング**により、利用者のデータがクラウドオペレーターから保護されている場合は、電気通信事業者がクラウドサービス上で通信の秘密に関する情報を取り扱ったとしても、**通信の秘密の侵害に当たらないことをガイドライン等で明確化**し、このような阻害要因を払拭していただきたく存じます。