

- 「AWS re:Invent 2021」特集
- 「Apache Log4j」の脆弱性について
- 新年のご挨拶

News Letter

2022.1
#09



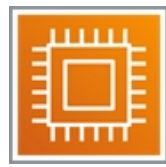
「AWS re:Invent 2021」特集

～AWS新サービス・アップデート情報紹介～

AWS re:Invent 2021が2021年日本時間の12月1日に行われました。今回は、このre:Inventで発表されたAWSの新サービスやアップデート情報について、一部抜粋してご紹介いたします。

AWS re:Inventとは？

AWS re:Inventは、米ラスベガスで毎年開催されているAmazon Web Services（AWS）のカンファレンスです。2021年は11月29日から12月3日（現地時間）の日程で開催され、日本からはオンデマンドでも視聴できました。毎年数多くの新サービスや新機能、アップデート情報などが発表される大注目のイベントです。



Compute & Containers



① EC2 Im4gn/Is4genインスタンス（新サービス）

ストレージ最適化インスタンス。

Im4gn：比較的安価なストレージ費用で利用可能。
データベースや分散ファイルシステムに最適。

Is4gen：CPUあたり最もストレージ容量が大きい。
大量データにランダムアクセスするような使い方に最適。

② EC2 G5gインスタンス（新サービス）

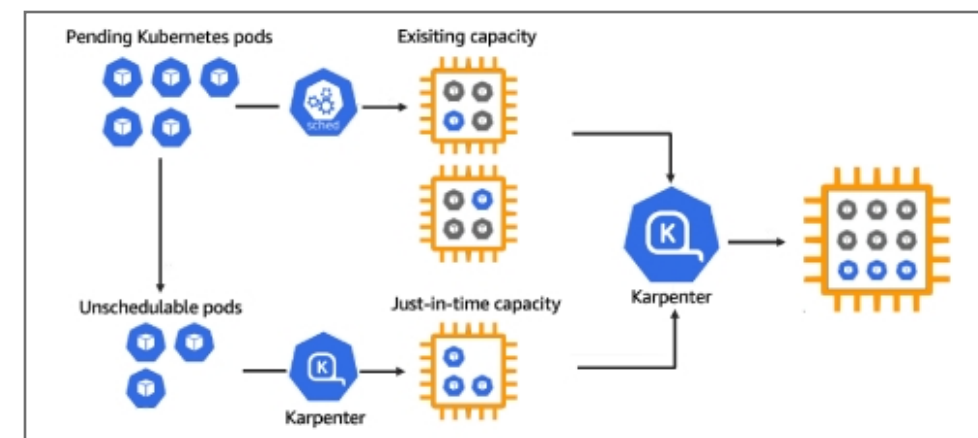
Android端末へのゲームストリーミング配信で費用対効果が高いインスタンス。
CPU処理の比重が大きく NVIDIA の AI ライブラリを活用するワークロードなどに最適。

③ EC2 M6aインスタンス（新サービス）

第3世代AMD EPYCプロセッサを搭載した汎用インスタンス。
M5aインスタンスと比較して最大35%の価格性能の向上、および同等のx86ベースのEC2インスタンスと比較して10%のコスト削減を実現。

④ AWS Karpenter v0.5（一般提供開始）

AWSで構築されたオープンソースのKubernetesクラスターオートスケーラー。アプリケーションの負荷の変化を監視し、状況に応じてインスタンスの追加・削除を実施。



⑤ AWS Compute Optimizer（アップデート）

コスト削減とパフォーマンス改善に関する2つのメトリクスを追加。

Savings Opportunity：推奨事項を適用することでEC2、EBS、Lambdaの費用をどの程度削減できるかを提示可能。

Performance Improvement Opportunity：アカウントレベルおよびリソースタイプレベルで、プロビジョニング不足のリソースの割合と数を定量化しボトルネックを可視化。



Storage

① Amazon S3 Glacier Instant Retrieval（新サービス）

即座にデータを取り出すことができるアーカイブ用途のAmazon S3の新しいストレージクラス。
メディアコンテンツのアーカイブ、ユーザ生成コンテンツ、医療画像、ゲノミクスなどの用途に最適。

コメント

スタンダードや標準IAのストレージクラスと同様のミリ秒単位で取得が可能な点もポイントです。
Glacier Instant Retrievalは四半期に一度程度のアクセスを想定しているので、すぐにアクセスする必要のあるアーカイブデータなどが主な対象になりそうですね。



② S3 Glacier Flexible Retrieval（アップデート）

S3 GlacierがS3 Glacier Flexible Retrievalへ名前を変更し、バルク取り出し費用の無料化や容量単価の10%値下げを発表。

③ Amazon S3で最大31%の値下げ（アップデート）

「S3 Standard-Infrequent Access」と「S3 One Zone-Infrequent Access」のストレージ価格を31%値下げ。
新価格は2021年12月1日より自動的に適用。

④ Amazon S3（アップデート）

Amazon S3のライフサイクルポリシーで保持する世代数と適用対象オブジェクトのフィルタリングが可能になり、コスト最適化にも有効。

⑤ Amazon EBS Snapshots Archive（新サービス）

EBSボリュームのスナップショットを長期保存するための新しいストレージ層。
90日以上保存する予定で、利用しない可能性が高いスナップショットのコストを最大で75%削減可能。

コメント

AWS管理下のS3バケットではなく、Archive Tier に保存することでコストダウンを可能にしたとのこと。
通常のスナップショット料金より75%割安になるので、リリース直前のバックアップイメージの保管など長期間保管が必要な場合に使える機能ですね。



⑥ Amazon EBS Snapshot ゴミ箱機能（新サービス）

EBSスナップショットの誤削除を防止するごみ箱機能が利用可能
EBSスナップショットを削除すると、Binと呼ばれるゴミ箱に移動するようになり、Bin内のスナップショットはポリシーに従って一定期間後に削除されるようになる。

⑦ Amazon FSx for OpenZFS（新サービス）

高速で低コストなフルマネージド型NFSファイルストレージサービス
ソフトウェアのビルド環境、機械学習環境などに最適。

⑧ AWS Backup for Amazon S3（アップデート）

AWS BackupがAmazon S3のバックアップに対応。
AWSアカウント全体のS3バケットとオブジェクトのバックアップとリ
ストアを一元的に管理可能。



Networking & Edge Service

① AWS Cloud WAN（新サービス）

グローバルなWide Area Network(WAN)を構築、管理、監視可能。
ネットワークの状態やセキュリティを可視化するダッシュボードを提供。



② Amazon VPC IP Address Manager（新サービス）

VPC上のIPアドレスを整理し、割り当て状態を管理するツール。
大規模なネットワークにおいて、IPアドレスを自動的に割り当てること
が可能。

③ Amazon VPC Network Access Analyzer（新サービス）

VPCリソースに意図しないネットワークアクセスがないかを簡単に特定
できる機能。
ネットワークアクセスがセキュリティやコンプライアンスのガイドライ
ンを満たしているかどうかを検証可能。



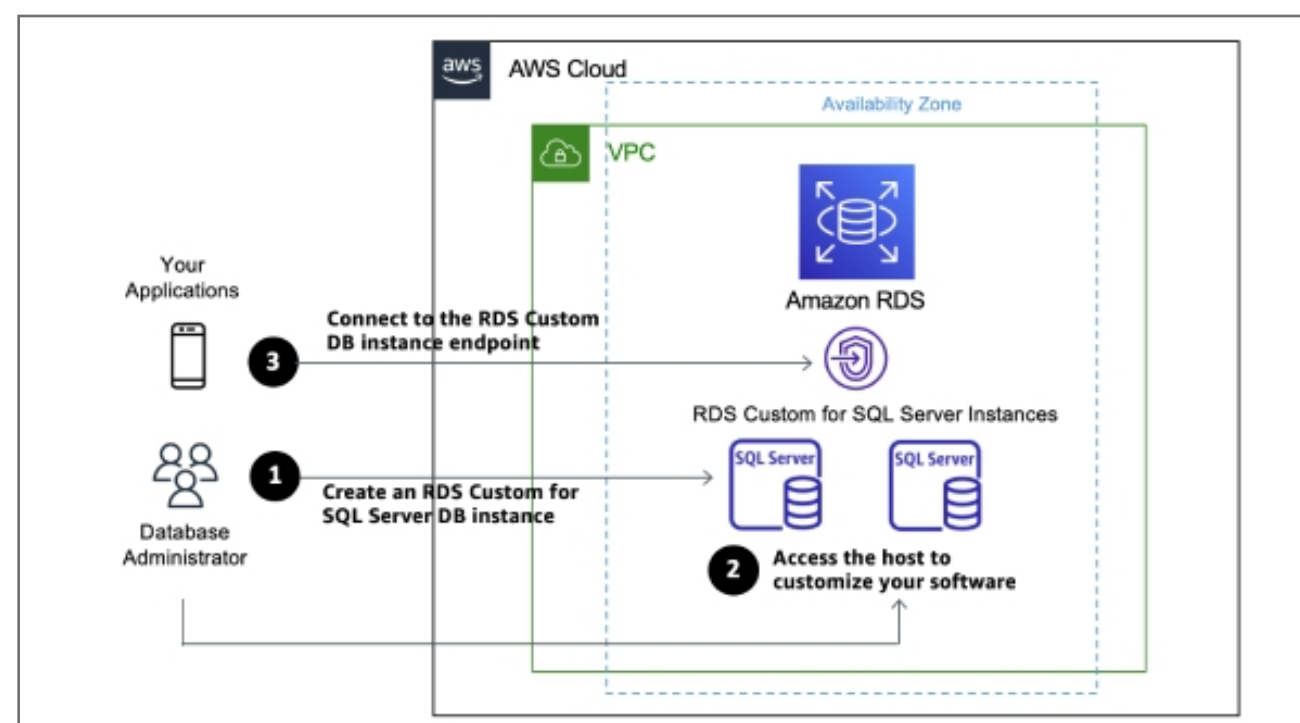
Database

① Amazon RDS Custom for SQL Server（新サービス）

DBサーバのOSやRDBMSの設定変更ができる。
従来はEC2で構築し自己管理が必要だったが、Amazon RDSのマネー
ジドサービスで対応可能に。

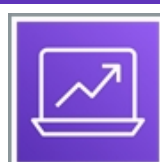
コメント

ユーザがデータベースやOSのパッチ適用、バックアップなどを含むメン
テナンスやカスタマイズ、OSへのSSHによるログインなどを実行可能に
なりました。ただ、あくまでAWSと共同で運用していくというスタンス
のため、AWS側から定期的に構成に対するチェックが入り、非サポート
となる構成を検出した場合はいくつかの操作が制限されるとのことです。
本番稼働するにはまだ検証が必要そうですね。



② Amazon DynamoDB

Amazon DynamoDBでストレージコストの削減を可能にする新しい
テーブルクラスであるStandard-IAテーブルクラスを追加。



Analytics

① Amazon EMR Serverless（アップデート）

ペタバイトクラスの大規模なデータ分析を簡単かつコスト効率高く実
行できる。
アプリケーションが必要とするリソースは自動的にプロビジョニング
及びスケーリングされ、使用したリソースに対してのみ料金を支払う。

② Amazon Kinesis Data Streams On-Demand（新サービス）

Kinesis Data Streamsの新しいキャパシティモードで、キャパシティ管
理なしで1分間にギガバイトの書き込みおよび読み込みが可能。



Artificial Intelligence & Machine Learning

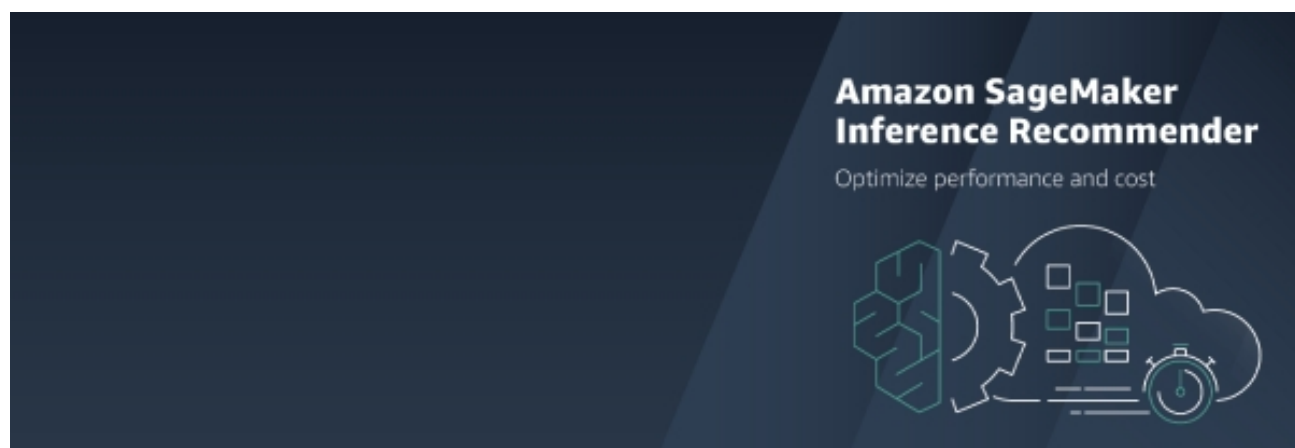
① Amazon SageMaker Serverless Inference（新サービス）

基礎となるインフラストラクチャを設定または管理することなく、推論用の機械学習モデルを簡単にデプロイすることができる新しいオプション。
推論リクエストの数に基づいて、処理能力を自動的にプロビジョニング、スケーリング、削除する。



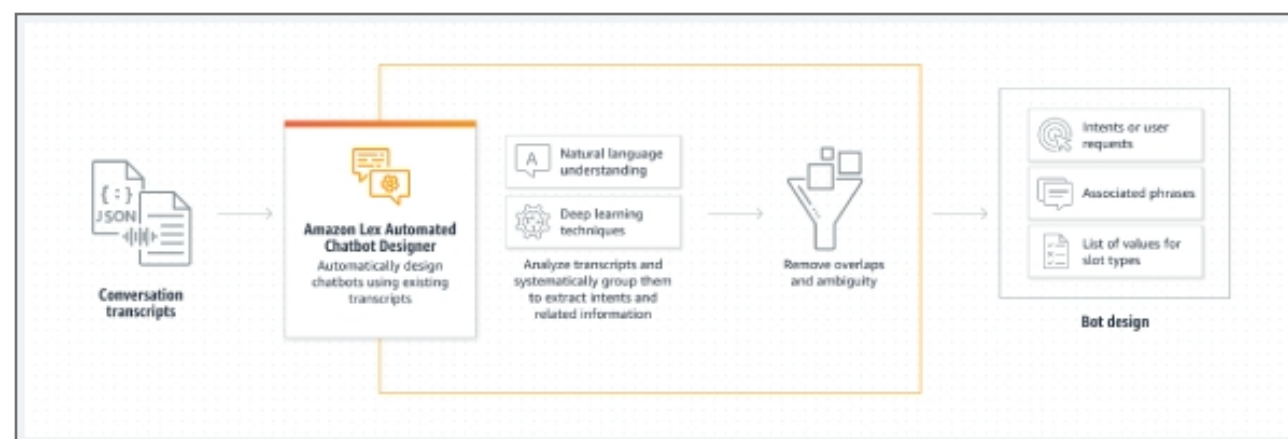
② Amazon SageMaker Inference Recommender（新サービス）

インスタンスタイプ、インスタンス数、コンテナパラメータ、及びモデルの最適化などの推奨項目を自動的に提示可能。



③ Amazon Lex Automated Chatbot Designer（新サービス）

機械学習を使用して、初期のボットデザインを提供。
開発者は過去の通話履歴を元に基本的なチャットボットを作成可能。



④ Amazon Personalize（アップデート）

レコメンド機能をこれまでよりも簡単に導入することが可能に。
タイミングに応じてユーザごとに異なるレコメンデーションを容易に設定可能。

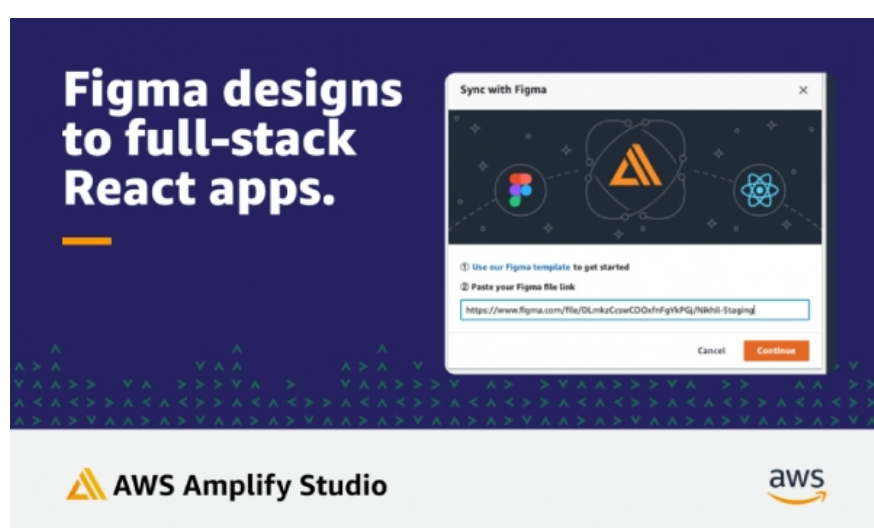


Developer Tools & Application Integration



① AWS Amplify Studio（新サービス）

Amplifyが提供するバックエンドの構成・管理機能と最小限のコーディングでUI開発を加速する新機能をフロントエンド開発者に提供するビジュアル開発環境。



② AWS Cloud Development Kit v2（新サービス）

デベロッパープレビューだったAWS CDK v2が一般提供開始。
プログラミング言語（TypeScript、Python、Java、C#、Go）のコードでAWS環境を構築・管理できるツールキット。

③ Amazon SQS（アップデート）

Amazon SQSの標準 キューにおいてDLQ(Dead Letter Queue)に入ったメッセージを元のキューに書き戻ることが可能に。



Security

① Amazon Inspector（アップデート）

継続的な脆弱性管理とリアルタイムに近い速度での脆弱性検知が可能に。
EC2インスタンスだけでなく、ECRに格納されたコンテナイメージについてもスキャンが可能。



Management & Governance

① Amazon CloudWatch RUM（新サービス）

Webアプリケーションのパフォーマンスをユーザサイドからモニタリングでき、ユーザ体験の改善に役立つReal-User Monitoring機能。

CloudWatch RUMを使用すると、異なるロケーション、ブラウザ、およびデバイス間でアプリケーションのパフォーマンスをほぼリアルタイムで確認でき、パフォーマンスの最適化が可能。

コメント

実際にユーザ側からみたパフォーマンスを確認し、インフラ側とアプリケーション側で原因の切り分けが可能になるのでWebアプリケーションの読み込み速度などのパフォーマンス改善に役立ちそうです。

② Amazon CloudWatch Evidently（新サービス）

A/Bテストやフィーチャーフラグといった手法でどちらの選択肢が望ましいか検証する際に、ユーザの挙動をモニタリングするサービス。

新UIやサーバサイドの挙動など、ビジネスに影響しうる要素変更・導入時にデータに基づいた良否の判断を可能にする。

コメント

ページロード時間の平均値やコンバージョン率をテストできるようになるので、すでに稼働しているアプリケーションへ新機能を追加する際に参考材料となりそうです。

③ Amazon CloudWatch Metrics Insights（新サービス）

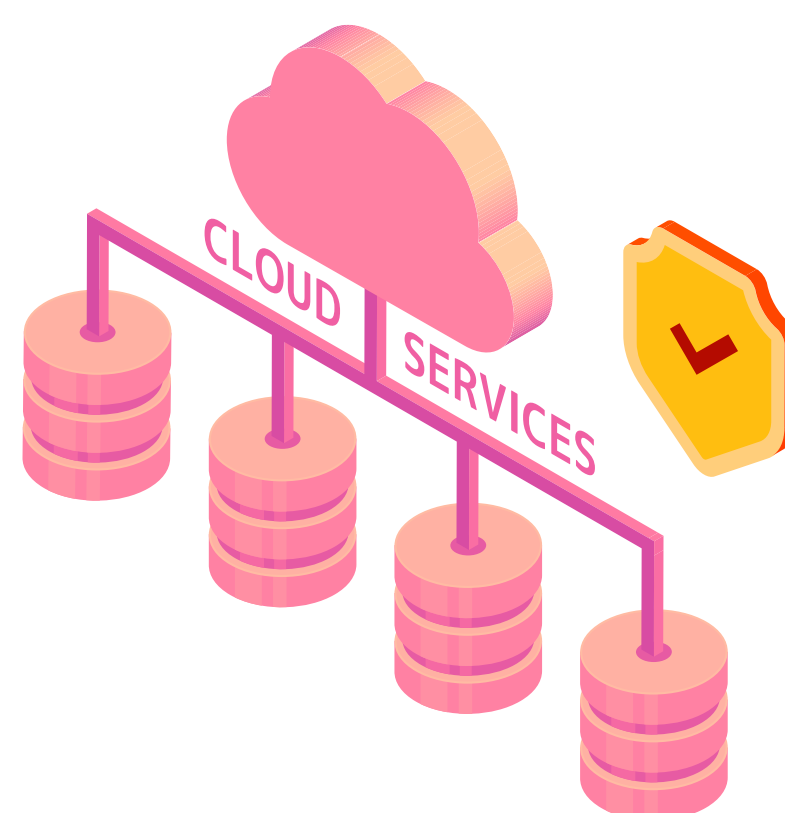
SQLベースのクエリによって、リアルタイムにCloudWatchメトリクスの集約やグループ化を行える新機能。

膨大な量のメトリクスからトレンドやパターンを見出すことが可能。

④ AWS Chatbot（アップデート）

AWS Chatbotを介して、Slack ChannelからAWS CLIのコマンドを発行し、AWSのリソースを管理可能。

例えば、EC2インスタンスのスケール、AWS Systems Managerランブックの実行、AWS Lambdaの同時実行制限の変更など。



Other

① AWS re:Post（新サービス）

AWSにおける技術課題を解決するためのQ&Aサービス。

AWSアカウントを持っていれば誰でも利用可能で、AWS利用者、パートナー、AWS従業員などのコミュニティから回答を受け取ることが可能。

③ Amazon QuickSight（アップデート）

Amazon QuickSightでIPアドレスベースでのアクセス制御が設定可能に。

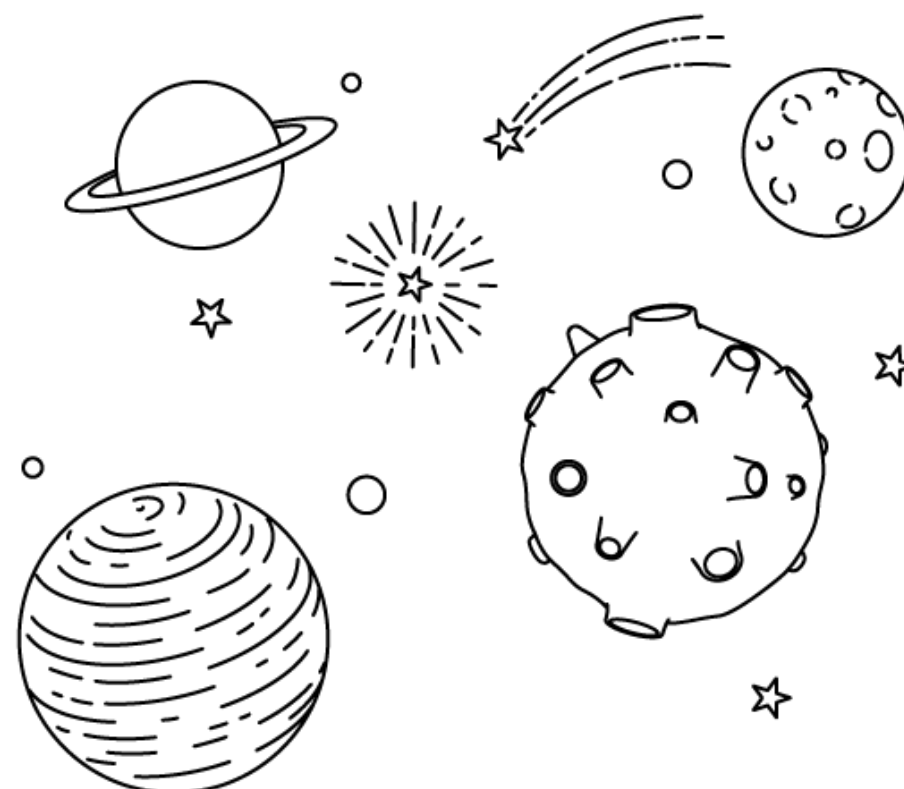
オフィスネットワークまたはVPN接続時のみアクセスできるというルールを実現可能。

② Amazon Linux2022 プレビュー開始

Amazon Linuxの最新OSとしてAmazon Linux2022のプレビューが開始2年ごとに新しくメジャーバージョンを提供し、各バージョンは5年間サポートされる。

コメント

現在のAmazon Linux 2はRHEL7をベースに、作られています。発表されたAmazon Linux2022はFedoraをベースに作られているとのこと。今後のバージョンアップスケジュールが2年ごと、またマイナーリリースは四半期ごと、サポート期間も明確に提示されているので、今後のスケジュールを立てやすくなりました。



2022年もAWSに期待

数多くの新サービスやアップデート情報をご紹介しましたが、気になるサービスはありましたでしょうか。今後もAWSの動向に注目していきましょう。ネットアシストでは、AWSに特化したマネージドサービスをご提供しております。ご興味のある方はお気軽に、ネットアシストへお問い合わせください。

「Apache Log4j」の脆弱性について

【1】log4jの脆弱性について（CVE-2021-44228）

2021年12月9日に公開されて以来、報道でも大きな話題となっている Apache Log4j の脆弱性についてご案内します。

本脆弱性は、「Apache Log4j」というJavaベースのロギングライブラリの機能を悪用する事によって、任意のコードが実行可能となる脆弱性です。例えば、脆弱性のある標的のサーバへ不正なHTTPリクエストを送信すると、任意のコマンドがリモートで実行され（＝RCE）、情報漏洩やデータの改ざんに繋がったり、サイバー攻撃の踏み台として悪用される可能性があります。

脆弱性の深刻度を評価するCVSS v3のスコアは最大の10.0（緊急）となっており、早急な対応が必要です。なお、Apache Log4j の「Apache」という点に関して、これはソフトウェア管理団体を示すものとなり、「Apache HTTP Server」を指すものではありません。

【2】脆弱性の対象

以下が脆弱性の対象となります（2022年1月5日時点）。

■対象

- ・ **Apache Log4j 2.15.0 より前の 2 系のバージョン**
 - ※Apache Log4j 2.12 系のうち 2.12.2 以降を除く
 - ※当初、Apache Log4j 1 系のバージョンは対象外だったが、特定の構成の場合は影響を受ける可能性があることが判明

▼任意のコードが実行可能な脆弱性(CVSSv3スコア,深刻度)
CVE-2021-44228 (10.0,緊急)

▼サービス運用妨害攻撃の脆弱性(CVSSv3スコア,深刻度)
CVE-2021-45046 (3.7,注意)

【3】脆弱性への対策方法

対策方法と回避方法は以下となります。

■対策方法

＜Java 8 及びそれ以降の場合＞

Log4j 2.17.0 以上へのアップデート

＜Java 7 の場合＞

Apache Log4j 2.12.3へのアップデート

■回避方法

JndiLookup クラスをクラスパスから削除する。

【4】弊社取扱サービスの状況

弊社が取り扱っているサービスに関する現状報告です。

■弊社取扱サービスの状況について

◎影響を受ける可能性のあったサービス ※影響なし

- ・ **改ざん検知サービス「WebARGUS」**

Javaベースのシステムで、保護対象サーバに Log4j ライブラリを含むエージェントが導入されますが、製品の仕様上、脆弱性を利用したリモートコード実行は不可能（影響を受けない）となっています。

Log4j ライブラリをアップデートする手法も用意されていますので、悪用される可能性は低くとも、今後導入されるお客様には、本脆弱性の対策を適用したエージェントを提供致します。

◎脆弱性リスクを低減できるサービス

- ・ **IPS/IDS「DeepSecurity IT Protection Service」**

Apache Log4jライブラリのアップデートや、不正な通信を受けないようにするコンテンツの改修等の対応をせずとも、仮想パッチでの暫定対処が可能となります。

以下の侵入防御 (DPI) ルールで本脆弱性に対応
ルール : 1011242 - Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)

- ・ **WAF「WafCharm」**

AWS WAF 環境にて、Apache Log4jの脆弱性を利用した攻撃に対応したルールを標準ルールに追加しました。また、難読化パターンの追加など継続的なルールのアップデートを順次実施しています。

- ・ **WAF「攻撃遮断くん」**

Apache Log4jの脆弱性を利用した攻撃を検知、遮断するシグネチャを追加しております。また、難読化パターンの追加など継続的なシグネチャアップデートを順次実施しています。

ただし、サーバセキュリティタイプについては、ログ解析によって遮断動作を行う仕様上、根本的な対策として、Apache Log4jライブラリのアップデートを実施していただくことをお勧めいたします。

【5】今後の情報にも注目

Apache Log4j の脆弱性に関しては、現在も日々情報がアップデートされています。最新情報については、IPA（独立行政法人情報処理推進機構）による以下のページも併せてご確認ください。

Apache Log4j の脆弱性対策について(CVE-2021-44228)

<https://www.ipa.go.jp/security/ciadr/vul/alert20211213.html>

ネットアシストのサービスをご利用されているお客様へ

「Apache Log4j」は弊社構築のサーバにて通常導入を行いませんが、TomcatやJBoss等、Javaを利用したサービスをお客様にて運用の際は、「Apache Log4j」を利用されている可能性がございます。誠に恐れ入りますが、お客様導入のアプリケーションは、ネットアシストの保守範囲外となります為、お客様にて確認をお願い致します。

新年のご挨拶

新年明けましておめでとうございます。



目指せ、猫から虎への進化！



皆様、新年明けましておめでとうございます。

伊藤でございます。

昨年はお客様、お取引先の皆様をはじめ関係各位には大変お世話になりました。誠に有難うございました。本年もどうぞ宜しくお願いいたします。

さて、今年は寅年ということで、ネコのマークでお馴染みのネットアシストのロゴを「寅バージョン」にしてみました。なんとなくタイガースっぽい雰囲気です。大阪営業所のロゴをこれに差し替えたなら売上が急伸するかもしれません。

そして寅年と言えましょう。寅年生まれの方は今年、年男を迎えました(12年ぶり4回目です)。4度目の年男イヤーとなる本年2022年は、一体どのような年になるのでしょうか？世界中で明るく楽しい話題が尽きず、皆が笑って過ごせるような素晴らしい年になることを切に願います。

今年は、私がネットアシストの代表に就任してから3年目の年になります。コロナ禍で世界が混沌とする中での船出でしたが、おかげ様で荒波に飲み込まれることもなく、業績は今のところ概ね好調です。

しかし振り返ってみますと、私自身が何か大きな力を発揮したという実感はあまり無く、周囲の皆さまから支えられ、押し上げられながら、曲がりなりにも何とかやってこられたな、という思いです。

お客様やお取引先様からのお力添えは言うに及ばず、部下である優秀な幹部陣や社員の面々が死力を尽くしてくれたからこそ今があるのだと、心の底から感謝しています。

「史記」からの故事成語に、

『雲は竜に従い風は虎に従う』

という言葉があります。これは、竜が雲を従え、虎が風を従えるように優れた天子(リーダー)の下には必ず優れた臣下(部下)が現れ、これをよく助ける、という意味です。まだまだ若輩の身で「優れた天子」とは程遠い私ですが、風を従えた虎のように、優秀な人材が次々と集ってくるようなリーダーを目指してこれからも人格の向上発展に努めていこうと思います。目指せ、猫から虎への進化！

それでは、本年もどうぞ宜しくお願い申し上げます。

株式会社ネットアシスト 代表取締役

伊藤誠史

お問い合わせ

株式会社ネットアシスト



03-3985-6780



sales@netassist.ne.jp



<https://www.netassist.ne.jp/>

