

SONY

マネージドクラウド  
新バージョンリリースのお知らせ  
Version 2.3.0

2023年9月28日

ソニービズネットワークス株式会社

# 目次

- マネージドクラウド with AWS
  - インスタンスセキュリティ機能拡張
    - NW（ネットワーク）到達性確認機能
    - レコメンデーション機能
    - パッチ適用テスト機能
    - SSMコマンドドキュメント改修
  - 月額AWS利用料金確定通知（概算料金 / 確定料金）機能
  - CloudTrail 既存証跡選択機能
  - イメージバックアップ復元時ネームタグ自動付与機能
- マネージド閉域接続サービス
  - レイアウト修正
- マネージドインターネットルータ
  - WAN回線変更
  - レイアウト修正

# マネージドクラウド with AWS

# インスタンスセキュリティ機能拡張

- ダッシュボードのインスタンス一覧において、NW（ネットワーク）到達性とTrusted Adviser レコメンデーションのモーダル表示を追加しました

The screenshot displays the AWS Management Console interface. At the top, there are tabs for 'Batch Compliance Summary' and 'Instances with the most urgent check results'. A modal window titled 'NW到達性' (Network Reachability) is open, showing a checkmark and the message 'Port 22 is reachable from an Internet Gateway - TCP'. Below this, it lists the components: InternetGateway, NetworkAcl, SecurityGroup, NetworkInterface, and Instance, each with a corresponding icon. Another modal window titled 'レコメンデーション' (Recommendations) is also open, displaying a table of recommendations. The table has three columns: '重要度' (Priority), '項目名' (Item Name), and '概要' (Summary). The first row shows a recommendation for '使用率の低い Amazon EC2 インスタンス' (Low utilization Amazon EC2 instances) with a 'Yellow' priority. The summary text explains that this recommendation checks for instances with low CPU utilization (below 10%) and high network I/O (above 5 MB) over the last 14 days. It also mentions that this can help reduce costs by identifying instances that can be terminated or scaled down. Below the table, there are sections for 'アラート基準' (Alert Thresholds) and '推奨されるアクション' (Recommended Actions), including links to Amazon EC2 monitoring and Auto Scaling documentation.

**NW到達性**

Port 22 is reachable from an Internet Gateway - TCP

InternetGateway:  
NetworkAcl:  
SecurityGroup:  
NetworkInterface:  
Instance:

**レコメンデーション**

重要度	項目名	概要
Yellow	使用率の低い Amazon EC2 インスタンス	直近 14 日間のいずれかの時間に実行した Amazon Elastic Compute Cloud (Amazon EC2) インスタンスをチェックし、1 日あたりの CPU 使用率が 10% 以下、およびネットワーク I/O が 5 MB 以下の日が 4 日以上あった場合は、アラートを通知します。インスタンスの実行には、1 時間ごとの使用料金が発生します。一部のシナリオでは仕様で使用量が低くなることもあります。インスタンスの数とサイズを管理することによってコストを削減できることがよくあります。

アラート基準

Yellow: 過去 14 日間のうち少なくとも 4 日間の間、インスタンスの 1 日あたりの平均 CPU 使用量が 10% 未満で、ネットワーク I/O が 5 MB 未満でした。

推奨されるアクション

使用率が低いインスタンスの停止もしくは終了を検討し、または Auto Scaling を使用してインスタンス数をスケールします。詳細については、「[インスタンスの停止と起動](#)」、「[インスタンスの終了](#)」、および「[Amazon EC2 Auto Scaling とは](#)」を参照してください。

追加のリソース

[Amazon EC2 のモニタリング](#)  
[インスタンスメタデータとユーザーデータ](#)  
[Amazon CloudWatch デベロッパーガイド](#)  
[Auto Scaling デベロッパーガイド](#)

# インスタンスセキュリティ機能拡張

- セキュリティジョブ管理のパッチ適用ジョブについて、「パッチ適用テスト」を行える機能を追加しました（適用の流れは後述）

TOP > AWS > サーバ管理 > インスタンスセキュリティ管理 > セキュリティジョブ管理 > セキュリティジョブ作成

## セキュリティジョブ作成

セキュリティジョブ名	<input type="text" value="セキュリティジョブ名"/>
ヘッダータイプ	<input type="text" value="ブルースカイ"/>
ジョブ	<input type="text" value="パッチ適用"/>
	<input type="radio"/> スキャンのみ実施
	<input type="radio"/> スキャン後、パッチのインストールを実施
	<input checked="" type="radio"/> スキャン後、パッチのテストを実施
	<input type="text" value="パッチ適用テスト通知先メールアドレス"/>
ターゲット	<input checked="" type="radio"/> リソースグループを指定
	<input type="text" value="リソースグループを選択"/>
	<a href="#">リソースグループを作成</a>

パッチ適用にテストを挟む場合の選択肢を追加。  
パッチ適用テスト用の環境構築の完了通知先を選択。

# インスタンスセキュリティ機能拡張

- パッチ適用テスト実施の流れについて

「パッチ適用テスト」の場合、ポータル側のバッチ処理実行基盤にて下記の一連の処理を実行します

Phase1. パッチ適用対象のEC2インスタンスの複製

- 複製元のAMIを取得
- AMIより、検証用のEC2インスタンスを構築 (ネットワーク, プロファイル等は複製元と同等)
  - 検証用インスタンス起動後、AMI削除
- 検証用インスタンスにてパッチ適用を実行。

Phase2. 検証用インスタンスにて顧客側で動作確認

- Phase1の処理完了後、顧客側へテスト環境の構築完了をメール通知
- 顧客側で検証インスタンスの動作チェック

ここまでで、一旦パッチ適用テスト処理を停止。  
待機状態となります。

Phase3. 本番環境への切り替え

- 承認モーダルで指定された方法で、本番へパッチ適用を反映させる
  - 検証インスタンスのEBSを本番インスタンスへと付け替える
  - 本番インスタンスにて改めてパッチ適用を実行する
- 切り替え処理完了後、もしくは切り替え実施しない場合、検証用のリソースを全て削除する

# インスタンスセキュリティ機能拡張

- パッチ適用テスト完了後、本番環境に対してパッチ適用の方法が選択できるようになります

TOP > AWS > サーバ管理 > インスタンスセキュリティ管理 > セキュリティジョブ管理

## セキュリティジョブ管理

リージョン選択 東京

### セキュリティジョブ一覧

ジョブ名	次回実行日時	操作
テスト	次回: 2023-08-13 00:00	実行 実行履歴 編集 削除
カスタムUPDA	次回: 2023-08-14 00:00	承認 実行履歴 編集 削除

### セキュリティジョブ承認

セキュリティジョブ「カスタムUPDATE」のパッチ適用テストを終了し、対象インスタンスへのパッチ適用を実行します。よろしいですか？

パッチ適用

- 対象インスタンスへパッチのインストールを実施する
- テスト済みインスタンスのEBSボリュームを対象のインスタンスへアタッチする
- テスト済みインスタンスを削除する

承認後のアクションを選択

対象インスタンス

キャンセル 実行

パッチ適用テストが待機状態となった場合、承認ボタンが表示されます。

# インスタンスセキュリティ機能拡張

- パッチ適用テスト実施後、本番環境へのパッチ適用方法について

「パッチ適用テスト」の場合、ポータル側のバッチ処理実行基盤にて下記の一連の処理を実行します

Phase1. パッチ適用対象のEC2インスタンスの複製

- 複製元のAMIを取得
- AMIより、検証用のEC2インスタンスを構築 (ネットワーク, プロファイル等は複製元と同等)
  - 検証用インスタンス起動後、AMI削除
- 検証用インスタンスにてパッチ適用を実行。

Phase2. 検証用インスタンスにて顧客側で動作確認

- Phase1の処理完了後、顧客側へテスト環境の構築完了をメール通知
- 顧客側で検証インスタンスの動作チェック

承認アクション後、パッチ適用処理を継続実行します。

Phase3. 本番環境への切り替え

- 承認モーダルで指定された方法で、本番へパッチ適用を反映させる
  - 検証インスタンスのEBSを本番インスタンスへと付け替える
  - 本番インスタンスにて改めてパッチ適用を実行する
- 切り替え処理完了後、もしくは切り替え実施しない場合、検証用のリソースを全て削除する



# インスタンスセキュリティ機能拡張

- セキュリティジョブ管理にて、任意のSSMコマンドドキュメントを実行できるように改修しました

TOP > AWS > サーバ管理 > インスタンスセキュリティ管理 > セキュリティジョブ管理 > セキュリティジョブ作成

## セキュリティジョブ作成

[お気に入り登録](#)

セキュリティジョブ名	<input type="text" value="セキュリティジョブ名"/>
ヘッダータイプ	<input type="text" value="ブルースカイ"/>
ジョブ	<input type="text" value="カスタム"/>

パッチ適用  
脆弱性スキャン  
✓ カスタム

ジョブ「カスタム」を追加

ドキュメント名	<input type="text" value="AWS-ApplyAnsiblePlaybooks"/>
SourceType	<input type="text" value="null"/>
SourceInfo	<input type="text" value="{}"/>
InstallDependencies	<input type="text" value="True"/>
PlaybookFile	<input type="text" value="hello-world-playbook.yml"/>
ExtraVariables	<input type="text" value="SSM=True"/>

SSMコマンドのドキュメント名を入力

ドキュメントに合わせて、パラメータ入力項目を表示

# 月額AWS利用料金確定通知（概算料金 / 確定料金）機能

- 月額AWS利用料金を月次でメール通知する機能を追加しました

TOP > AWS > 利用料金 > AWS利用料金 > AWS利用料金設定

## AWS利用料金設定

お気に入り登録

月次課金情報 月次メール通知設定

基本設定	設定内容		
月次課金情報の月次メール通知設定	送信ポリシー	全て送信する	編集
	送信先アドレス		
	集計対象AWSアカウント		

基本設定	設定内容		
月次課金情報の月次メール通知設定	送信ポリシー	全て送信する	送信しない 概算のご請求金額のみ送信する 確定のご請求金額のみ送信する ✓ 全て送信する
	送信先アドレス		
	集計対象AWSアカウント	<input checked="" type="checkbox"/> 362020 <input checked="" type="checkbox"/> 202205	

戻る 設定

毎月8日 09:00 に月次メール発報

- 概算のご請求金額
  - 前月の概算金額（速報料金）を通知  
※金額修正が入る場合があるため未確定金額となります
- 確定のご請求金額
  - 前々月の確定金額を通知

# CloudTrail 既存証跡選択機能

- IAMユーザー申請のIAM操作アラートについて、利用する証跡を選択できるように改修しました

TOP > AWS > IAMユーザー申請 > IAMユーザー利用許可申請

## IAMユーザー利用許可申請

お気に入り

承認者

有効期限

希望権限

リージョン制御

IAM操作アラート通知

通知先選択   
AWS SNS Topic の作成は [こちら](#)  
※ ヴァージニアリージョンに作成する必要があります

ポータル管理の証跡を利用  
 既存の証跡を利用

CloudTrail証跡  
既存の証跡を利用する設定について  
・ 既存の証跡を用いてIAM操作アラート通知を開始するために、本設定の保存後、各種設定を行う必要があります。ヴァージニアリージョンに既存の証跡が存在しない場合は選択できません。  
- 選択した証跡のログ記録を開始します。  
- 選択した証跡の管理イベントを、API アクティビティの書き込みにチェックが入ったまま ON にします。

利用する証跡を選択可能化。  
既存証跡を利用する場合、必要な設定項目を表示。  
(ユーザー側で設定を導入。)

# CloudTrail 既存証跡選択機能

- AWSログ監査の異常操作アラートについて、利用する証跡を選択できるように改修しました

**AWSログ監査 異常操作アラート通知設定**

異常操作アラート通知では、各種AWSリソースにおいて異常な操作を検出し、指定トピックへアラートを通知します。

監視対象リージョン 東京

異常操作監視  有効  無効

通知トピック 通知先を選択

CloudTrail証跡

ポータル管理の証跡を利用

既存の証跡を利用 ? portal-resource-audit

既存の証跡を利用する設定について

- ・既存の証跡を用いて異常操作アラート通知を開始するために、本設定の保存後、各種設定を行う必要があります。既存の証跡が存在しない場合は選択できません。
- 選択した証跡のログ記録を開始します。
- 選択した証跡のCloudWatch Logsを有効化します。
- CloudWatch Logsのロググループ名では既存を選択し、「portal-cloud-trail-insight-log-group」と入力します。
- CloudWatch Logsのロール名では既存を選択し、「portal-cloud-trail-role」を選択します。
- 選択した証跡の管理イベントを、API アクティビティの読み取り・書き込みにチェックが入ったままONにします。

キャンセル 設定

利用する証跡を選択可能化。  
既存証跡を利用する場合、必要な設定項目を表示。  
(ユーザー側で設定を導入。)

# CloudTrail 既存証跡選択機能

- MSSリソース監査のCloudTrail設定について、利用する証跡を選択できるように改修しました

TOP > AWS > マネージドサポート管理 > リソース監査設定

## リソース監査設定

### AWS CloudTrail有効化設定

AWS CloudTrailにて証跡を作成します。  
全リージョン有効化する場合は東京リージョンにてすべてのリージョンに適用される証跡を作成し有効化します。

バケット名

保存期間

全リージョン有効化  有効  無効

CloudTrail証跡  ポータル管理の証跡を利用  既存の証跡を利用

既存の証跡を利用する設定について

- 既存の証跡を用いてリソース監査を開始するために、本設定の保存後、各種設定を行う必要があります。既存の証跡が存在しない場合は選択できません。
- 選択した証跡のログ記録を開始します。
- 選択した証跡がマルチリージョン対応証跡の必要があります。

キャンセル 設定

利用する証跡を選択可能化。  
既存証跡を利用する場合、必要な設定項目を表示。  
(ユーザー側で設定を導入。)

# イメージバックアップ復元時ネームタグ自動付与機能

- イメージバックアップのリストア実行において名称指定がない場合、バックアップ取得時のNameタグをEC2インスタンスに転記するように改修しました

リストア実行

このAMIから新規インスタンス立上（リストア）を実行します。  
立上時に必要な下記項目を指定して下さい。  
※本機能では現状インスタンスと同じIPアドレスの指定はできません。

サブネット

eth0

サーバ名

**！注意事項！**

- ・リストア実行後、新たにインスタンスが作成され古いインスタンスは削除されません。
- ・新たなインスタンスは以前設定されていた様々な設定が初期化されるため、必ず改めて再設定をお願いいたします。

一例)

- ・CPUやメモリ等の閾値通知設定、電源ON/OFF設定
- ・スナップショット、イメージバックアップ等のスケジュール設定
- ・リモート管理設定
- ・自動復旧アクション設定

キャンセル

名称未指定時はバックアップ取得時のNameタグを利用してリストア

# マネージド閉域接続サービス

# レイアウト修正

- 以下の画面で軽微なレイアウト修正をおこないました
  - 基本契約情報管理
  - マネージド閉域ルータ FW設定
  - マネージド閉域ルータ DHCP設定
  - マネージド閉域ルータ ルーティング設定



# マネージドインターネットルータ

# WAN回線変更

- 利用拠点を解約せずにルータ設定を維持したままWAN回線を変更できる機能を追加しました  
※WAN回線変更をご希望される際は、弊社担当営業までご連絡ください

# レイアウト修正

- 以下の画面で軽微なレイアウト修正をおこないました
  - 基本契約情報管理
  - マネージドインターネットルータ FW設定
  - マネージドインターネットルータ DHCP設定
  - マネージドインターネットルータ ルーティング設定

# SONY

SONYはソニー株式会社の登録商標または商標です。

各ソニー製品の商品名・サービス名はソニー株式会社またはグループ各社の登録商標または商標です。その他の製品および会社名は、各社の商号、登録商標または商標です。