

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 2.2.0

2023年6月26日

ソニービズネットワークス株式会社

- マネージドクラウド with AWS
  - AWSアカウント初期表示設定及び視認性向上
  - AWS利用料金複数アカウント合算通知機能追加
  - インスタンスセキュリティ管理機能追加
  - GLB管理機能追加

# マネージドクラウド with AWS

# AWSアカウント初期表示設定及び視認性向上

- 複数AWSアカウント契約がある場合、ユーザー毎に「デフォルトで表示するアカウント」及び「アカウント毎のカラー」を設定できるようにしました

The screenshot displays the Managed Cloud Portal interface. A modal dialog titled '各種アカウント設定' (Account Settings) is open, allowing users to configure account information. The dialog includes a title bar with a close button (X) and a main area with the following text:

各種アカウント情報を設定します。  
各種アカウント名の設定が存在しない場合は、各種アカウントID (AWSアカウント, Azureドメイン) のみクラウドポータルに表示されます。

**AWS**

AWSアカウント	AWSアカウント名	デフォルト	カラー
	いつもの環境	<input checked="" type="radio"/>	
	ダミー	<input type="radio"/>	

Buttons: キャンセル, 設定

Below the dialog, the 'AWSアカウント' dropdown menu is visible, showing 'いつもの環境' as the selected option. Below it are buttons for '切り替える' and 'アカウント設定を変更'.

# AWS利用料金複数アカウント合算通知機能追加

- 複数AWSアカウント契約がある場合、料金合算で各種アラート監視できるようにしました

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

### AWS利用料金 アラート通知設定

アラート名	利用額	通知先トピック	集計対象サービス	集計対象AWSアカウント	削除
PortalCEAlert20230613151427	300(USD)	PortalTopic-tasaki-test_20211209_175649	全てのサービス	36202 20220	削除

アラート通知設定

### AWS利用料金

基本設定

AWS利用料金の週次メ

#### AWS利用料金 アラート通知設定

利用額 \$ 3000

集計対象AWSアカウント

- 36202
- 20220

集計対象サービス

- 全てのサービス
- AWS Application Migration Service
- AWS CodePipeline
- AWS Config
- AWS Cost Explorer

リージョン 東京

通知先トピック

トピック PortalTopic-iriko\_TEST\_20230214\_142726

キャンセル 設定

編集

日, 11:00に通知する。

# AWS利用料金複数アカウント合算通知機能追加

- 複数AWSアカウント契約がある場合、料金合算で各種アラート監視できるようにしました

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

### AWS利用料金 アラート通知設定

アラート名	利用額
PortalCEAlert20230613151427	300(USD)

アラート通知設定

### AWS利用料金 週次メール通知設定

基本設定	設定内容
AWS利用料金の週次メール通知設定	送信ポリシー <input type="radio"/> 送信しない <input checked="" type="radio"/> 送信する
	送信先アドレス
メール通知スケジュール	曜日指定 <input type="radio"/> 日曜日 <input type="radio"/> 月曜日 <input type="radio"/> 火曜日 <input type="radio"/> 水曜日 <input type="radio"/> 木曜日 <input checked="" type="radio"/> 金曜日 <input type="radio"/> 土曜日
	時間指定 11時 00分

戻る 設定

基本設定	設定内容
AWS利用料金の週次メール通知設定	送信ポリシー 送信する
	送信先アドレス
集計対象AWSアカウント	36202 , 20220
メール通知スケジュール	毎週金曜日, 11:00に通知する。

編集

# インスタンスセキュリティ管理機能

- EC2に関するセキュリティ情報をダッシュボードに集約して一括表示できるようにしました

The screenshot displays the AWS IAM console dashboard for instance security. It features several key sections:

- バッチコンプライアンス概要**: A donut chart showing compliance status for batch instances.
- 最も緊急の検出結果があるインスタンス**: A table listing instances with the most critical findings.
- 外部公開されているインスタンス**: A summary card showing 3 instances.
- 24時間以内に検出された脅威のリスト**: A table of threats detected within the last 24 hours.
- レコメンデーション**: A section with recommendations for improving instance security.
- インスタンス一覧**: A grid of instance cards, each with a security score and status indicators for various checks.

インスタンス ID	AWS アカウント	AMI ID	緊急	すべて
		ami-54294c19	18	517
		ami-cc01be6	17	647
		ami-2724c5f8	7	191
		ami-0b75464839d7acc12	0	1
		ami-072bfb8ac2c884cc4	0	176

検出タイプ	重要度
Policy:IAMUser:RootCredentialUsage	Low
Policy:IAMUser:RootCredentialUsage	Low
Stealth:IAMUser:CloudTrailLoggingDisabled	Low

3
---

インスタンスを対象としているレコメンデーション
● EC2 インスタンスは AWS Systems Manager によって管理される必要があります
● Systems Manager によって管理される EC2 インスタンスは、パブリックインスタンスにバッチコンプライアンスのステータスが [COMPLIANT] である必要があります

インスタンス名	セキュリティレポート
Portal踏み台	1
Portal-001	2
PortalNAT	3
Docker動作確認くん	4
ADテストWindo...	5
aws01mnrsv01d	6

# インスタンスセキュリティ管理機能

【事前設定】 インスタンスセキュリティ機能をご利用いただく前に各基本設定を実施してください

TOP > AWS > サーバ管理 > インスタンスセキュリティ管理 > 基本設定

## 基本設定

お気に入り登録

🔍 絞り込み検索

+ 開く

Guard Duty

Guard Duty基本設定よりGuard Dutyを有効化してください。

Inspector v2

有効  無効

Patch Manager

リモート管理, セキュリティジョブ管理より各インスタンスのパッチ適用を設定してください。

設定

# インスタンスセキュリティ管理機能

【事前設定】サーバーリモート画面から予め「パッチ適用」と「脆弱性スキャン」を設定してください

TOP > AWS > サーバ管理 > リモート管理 > SYSTEM MANAGER設定 > コマンド登録

コマンド登録 お気に入り登録

設定内容

実行内容	
SSMコマンド種別	
実行パラメーター	<pre>Components :[   {     "Id": "ApplicationEventLog",     "FullName": "AWS.EC2.Windows.CloudWatch.EventLog.EventLogInputComponent,AWS.EC2.Windows.CloudWatch",     "Parameters": {       "LogName": "Application",       "Levels": "1"     }   } ]</pre>

自分で編集する

戻る 設定

▼ メモリ/ディスク監視追加

ドライブレター情報取得

EC2Configアップデート

SSM エージェントアップデート

CloudWatch エージェントインストール

Replication エージェントインストール

Inspector エージェントインストール

WindowsUpdate 更新確認

WindowsUpdate インストール

パッチ適用

脆弱性スキャン

パワーシェル実行

# インスタンスセキュリティ管理機能

- メイン画面ヘッダー情報部分の各詳細情報について

**パッチコンプライアンス概要**

■ 標準  
■ 重要な非準拠  
■ 高い非準拠  
■ その他非準拠

高い非準拠 3  
その他非準拠 3

**最も緊急の検出結果があるインスタンス**

インスタンス ID	AWS アカウント	AMI ID	緊急	すべて
		ami-54294cb9	18	517
		ami-ceafcb8	17	647
		ami-2724cf58	7	191
		ami-0b7546e839d7ace12	0	1
		ami-072bfb8ae2c884cc4	0	176

※上位5つまでのインスタンスを表示しています。

**外部公開されているインスタンス**

3

**24時間以内に検出された脅威のリスト**

検索タイプ	重要度
Policy:IAMUser/RootCredentialUsage	Low
Policy:IAMUser/RootCredentialUsage	Low
Stealth:IAMUser/CloudTrailLoggingDisabled	Low

**レコメンデーション**

インスタンスを対象としているレコメンデーション

- EC2 インスタンスは AWS Systems Manager によって管理される必要があります
- ✖ Systems Manager によって管理される EC2 インスタンスは、パッチのインストール後にパッチコンプライアンスのステータスが [COMPLIANT] である必要があります

**外部からのネットワークパスがあるインスタンス数を表示。(Inspector v2 での Network Reachability の指摘)**

**緊急性のある脆弱性を含むインスタンスを表示(Inspector v2)**

**直近で検出されたAWSアカウントの脅威リストを表示。(Gurad Duty)**

**インスタンスを対象とした推奨事項を表示。(Trusted Advisor)**

# インスタンスセキュリティ管理機能

- メイン画面インスタンス毎表示部分の各詳細情報について

The screenshot displays the 'インスタンス一覧' (Instance List) page. At the top left is a search bar with the text '絞り込み検索' (Filter Search). At the top right is a '+ 開く' (Open) button. Below the search bar is a 'セキュリティレポート' (Security Report) section with a dropdown menu showing '1', '2', '3', and a '1ページの表示件数: 6' (Number of items displayed per page: 6) dropdown.

The main area contains a grid of instance cards. Each card has a title, a chip icon, and a status bar with three indicators: '脅威検知' (Threat Detection), '脆弱性' (Vulnerability), and '未適用パッチ' (Unapplied Patches). Below each card are 'NW到達性' (Network Reachability) and 'レコメンデーション' (Recommendation) status indicators.

Three callout boxes provide detailed information:

- 対象インスタンスの脆弱性サマリ** (Vulnerability Summary for Target Instance): A donut chart showing the distribution of vulnerabilities by severity. The legend includes 'HIGH', 'MEDIUM', 'CRITICAL', and 'LOW'. The chart shows a large 'MEDIUM' section and a smaller 'HIGH' section.
- 対象インスタンスの脅威サマリ** (Threat Summary for Target Instance): A donut chart showing the distribution of threats by severity. The legend includes 'High', 'Medium', and 'Low'. The chart is almost entirely red, indicating a high level of threat.
- 対象インスタンスのパッチ適用状況サマリ** (Patch Application Status Summary for Target Instance): A donut chart showing the distribution of patch application status. The legend includes '最新パッチ適用' (Latest Patch Applied), '古いパッチ適用' (Old Patch Applied), and '未パッチ適用' (No Patch Applied). The chart is mostly yellow, indicating that most instances have old patches applied.

At the bottom right, there is a 'セキュリティレポート画面に遷移' (Move to Security Report Screen) button.

# インスタンスセキュリティ管理機能

- セキュリティ情報レポートを定期的に出力するための設定画面

TOP > AWS > サーバ管理 > インスタンスセキュリティ管理 > ダッシュボード > セキュリティレポート

## セキュリティレポート

お気に入り登録

### レポート設定

閉じる

曜日設定/日にち設定  設定なし  曜日設定する  日にち設定する

曜日指定  日曜日  月曜日  火曜日  水曜日  木曜日  金曜日  土曜日

時間指定

保存先S3バケット

通知先メールアドレス

設定

セキュリティレポートの

- ・ 作成日時
- ・ 保存先のS3バケット (顧客AWSアカウント)
- ・ レポート作成の通知先
  - ・ メールにてダウンロードリンクを通知を指定。

### レポート一覧

選択項目を削除 選択項目をダウンロード 1ページの表示件数: 10 S3バケット: amazon-connect-7dcadba9e28e

レポート名	タイムスタンプ	
security_report_20230614131807.html	2023/06/14	<input type="checkbox"/>
security_report_20230613131807.html	2023/06/13	<input type="checkbox"/>
security_report_20230612131814.html	2023/06/12	<input type="checkbox"/>

1 2 3 ... → →

レポート一覧の確認やダウンロードが可能

# インスタンスセキュリティ管理機能

## レポート出力例

インスタンスセキュリティレポート					
発行日：2023/06/14					
Section1: サマリ					
未適用バッチ数					
インスタンス名	インスタンスID	Important	Medium	Low	
Portal-002		64	0	0	
vulnerability_test_instance_2		0	0	0	
脆弱性数					
インスタンス名	インスタンス名	Critical	High	Medium	Low/Informational
Portal-002		18	239	228	32
Portal踏み台		17	275	298	57
アクティブな脅威数					
High	Medium			Low	
0	2			2	
Section2: インスタンス別詳細					
インスタンス毎のバッチ・脆弱性・脅威の一覧です。					
Portal-002					
未適用バッチ一覧					
バッチ名	分類	重要度	説明	ステータス	
bind-export-libs.x86_64	Security	Important	bind-export-libs.x86_64:32:9.11.4-26.p2.amzn2.13	Missing	
bind-libs.x86_64	Security	Important	bind-libs.x86_64:32:9.11.4-26.p2.amzn2.13	Missing	
bind-libs-lite.x86_64	Security	Important	bind-libs-lite.x86_64:32:9.11.4-26.p2.amzn2.13	Missing	

# インスタンスセキュリティ管理機能

- EC2に関するセキュリティパッチ適用設定を一括管理できるようにしました

(事業部門利用) ビットドライブ: | 権限: 全体管理者 | AWSアカウント: (いつもの環境) ログアウト

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

お気に入り登録

絞り込み検索 + 開く

1ページの表示件数: 12

ジョブ名	次回実行日時	操作
バッチ適用 (インストー)	次回: -	実行, 実行履歴, 編集, 削除
バッチ適用ジョブ 1 (...)	次回: 2023-07-01 00:00	実行, 実行履歴, 編集, 削除
SSIETEST99...	次回: 2023-07-01 00:00	実行, 実行履歴, 編集, 削除
SIETEST	次回: -	実行, 実行履歴, 編集, 削除
SIETEST_002	次回: 2023-07-01 00:00	実行, 実行履歴, 編集, 削除
SIETEST_003	次回: 2023-07-01 00:00	実行, 実行履歴, 編集, 削除

セキュリティジョブを追加

セキュリティジョブの新規作成/編集画面へ遷移

# インスタンスセキュリティ管理機能

【事前設定】 予め定期チェックするためのジョブを作成してください

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

ヘッダータイプ

ジョブ

スキャンのみ実施

スキャン後、パッチのインストールを実施

パッチインストール後の再起動を容認しない

ターゲット

リソースグループを指定

インスタンスを指定

Portal踏み台

Service踏み台

Portal-001

Service-001

PortalNAT

通知先

スケジュール  設定なし

曜日設定

日にち設定

ブルースカイ  
オレンジ  
ワインレッド  
リーフグリーン

パッチ適用  
脆弱性スキャン

ジョブ種別とオプションを指定

リソースグループ or インスタンスを指定(複数可)

実行スケジュールを指定

# インスタンスセキュリティ管理機能

## ● セキュリティチェックに関する設定画面

The screenshot shows the AWS IAM console interface for managing security jobs. At the top, there are navigation breadcrumbs: (事業部門利用) ビットドライブ: > 権限: 全体管理者 > AWSアカウント: (いつもの環境) > ログアウト. Below this is the page title "セキュリティジョブ管理" and a search icon with the text "お気に入り登録".

An orange callout box highlights the text "ジョブを即時実行" (Run job immediately). Below this, a modal dialog titled "セキュリティジョブ即時実行" (Run security job immediately) is open. The dialog contains the following information:

- セキュリティジョブ「SIETEST」を即時実行します。よろしいですか？
- ジョブ: バッチ適用
- オプション: スキャンのみ実施
- 対象インスタンス: (empty)

At the bottom of the dialog are two buttons: "キャンセル" (Cancel) and "実行" (Run). The "実行" button is highlighted with an orange arrow pointing from the callout box.

The background page shows a list of security jobs. The first job is "SIETEST" with a next run time of "-". The second job is "SIETEST\_002" with a next run time of "2023-07-01 00:00". The third job is "SIETEST\_003" with a next run time of "2023-07-01 00:00". Each job card includes a lightning bolt icon for "実行" (Run) and a clock icon for "実行履歴" (Execution history), along with "編集" (Edit) and "削除" (Delete) buttons. A "1ページの表示件数: 12" (Items per page: 12) dropdown is visible on the right.

At the bottom left of the page, there is a button labeled "セキュリティジョブを追加" (Add security job).

# インスタンスセキュリティ管理機能

## ● セキュリティチェックに関する実行履歴画面

(事業部門利用) ビットドライブ: | 権限: 全体管理者 | AWSアカウント: (いつもの環境) ログアウト

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

絞り込み検索

ジョブの実行履歴を表示

お気に入り登録

#### セキュリティジョブ実行履歴

2023-05-11 13:00:00				閉じる
2023-05-11 13:07:00	完了	バッチ適用	実行完了	詳細
2023-05-11 13:07:00	完了	バッチ適用	実行完了	詳細
2023-05-11 13:02:09	失敗	バッチ適用	EC2インスタンスが停止中/EC2リモート管理対象外によるエラー	詳細
2023-05-12 14:00:00				開く
2023-05-11 14:00:00				開く
2023-06-14 17:00:00				開く
2023-05-24 13:00:00				開く
2023-05-22 15:00:00				開く

セキュリティジョブを追加

# GLB管理機能追加

- ELBの一種であるGLBを管理する機能を追加しました

ELB一覧 更新

東京

ALB	基本情報	セキュリティグループ	アクセスログ	ターゲットグループ			
				ターゲット構成	ヘルスチェック	リスナー	運用監視
 20210604	internet-facing VPC: vpc-  <AZ> ap-northeast-1c ap-northeast-1a ap-northeast-1d	launch-wizard-2	無効  <a href="#">設定</a>	20210604-alb  インスタンスが存在しません。	<a href="#">表示</a>	<a href="#">表示</a>	<a href="#">詳細</a>

各種ツールチップ, 運用監視表示は他LBと同等

GLB	基本情報	セキュリティグループ	ターゲットグループ			
			ターゲット構成	ヘルスチェック	リスナー	運用監視
 glb-test-20230522	VPC: vpc-  <AZ> ap-northeast-1d ap-northeast-1a ap-northeast-1c	-	glb-test  ELFE_2.2.0_CPU  unhealthy	<a href="#">表示</a>	<a href="#">表示</a>	<a href="#">詳細</a>

# 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。