

パートナークラウドサービス(A)

別紙 セキュリティ監査サービス

Ver. 1.0.2

目次	
1. セキュリティ監査サービス	- 4 -
1.1. サービス概要	- 4 -
1.2. サービス内容	- 4 -

変更履歴

版数	変更年月日	変更内容
1.0.0	2021/9/30	初版作成
1.0.1	2022/10/1	監査項目の最新化に伴い、セキュリティポリシールールを別紙にて作成
1.0.2	2025/3/3	情報所有者の変更

1. セキュリティ監査サービス

1.1. サービス概要

お客様 AWS 環境に対し、セキュリティ監査項目に準拠しているかの監査を定期的の実施します。

1.2. サービス内容

仕様項目	内容																				
サービス内容	お客様 AWS 環境に対し、セキュリティ監査項目に準拠しているかの監査を定期的の実施します。 お客様 AWS 環境の設定を当社監査環境で取得し、定期的な監査の結果、監査ルール違反/問題がある場合にお客様指定メールアドレスに通知します。																				
提供方法	・PCS ポータルよりの問合せフォームより、監査対象リージョン・通知先情報を回答し、本サービスに申し込み頂きます。 ・申し込み後、下記「前提条件・制約条件」に記載している AWS 設定項目の設定作業を実施します。 ・サービス提供までのリードタイムはアカウント発行 5 営業日、セキュリティ監査サービスの個別見積対応および設定作業 10 営業日が目安となります。																				
監査対象	お客様 AWS 環境の全リージョン(マルチアカウント対応)																				
監査間隔	日次で監査を実施します。																				
前提条件・制約事項	1. 本サービスでは AWS Config を利用します。(利用者側で設定した AWS Config は当サービスでは検知不可) 2. AWS 設定項目 監査を実施するにあたり AWS Config の機能を利用します。 お客様 AWS 環境で以下の項目を有効にさせて頂く必要があります。 <table><tr><th>項番</th><th>必要項目</th><th>概要</th><th>担当者</th></tr><tr><td>1</td><td>Execution Role 作成</td><td>CloudFormation を利用して、ソースアカウント側に ExecutionRole (Stacksets の実行を許可するための IAM ロール)を作成します。</td><td>利用者</td></tr><tr><td>2</td><td>AWS Configログ保存用 S3 バケット構築</td><td>AWS の設定履歴、設定スナップショットを保存するための S3 バケットを用意します。</td><td>構築担当者</td></tr><tr><td>3</td><td>AWS Config 有効化</td><td>全リージョンの AWS Config を有効化します。</td><td>構築担当者</td></tr><tr><td>4</td><td>AWS Config アグリゲータ承認</td><td>当社監査環境との AWS Config 接続を承認します。</td><td>構築担当者</td></tr></table> 3. 通知用メールアドレス 監査ルール違反/問題がある場合にメールにて通知します。通知先のメールアドレスをご用意ください。 4. サービス利用対象者 本サービスは申込者が NTT データ社内の場合のみ提供可能です。 また、新規アカウントが対象となるため、既存の利用者は別途ご相談ください。	項番	必要項目	概要	担当者	1	Execution Role 作成	CloudFormation を利用して、ソースアカウント側に ExecutionRole (Stacksets の実行を許可するための IAM ロール)を作成します。	利用者	2	AWS Configログ保存用 S3 バケット構築	AWS の設定履歴、設定スナップショットを保存するための S3 バケットを用意します。	構築担当者	3	AWS Config 有効化	全リージョンの AWS Config を有効化します。	構築担当者	4	AWS Config アグリゲータ承認	当社監査環境との AWS Config 接続を承認します。	構築担当者
項番	必要項目	概要	担当者																		
1	Execution Role 作成	CloudFormation を利用して、ソースアカウント側に ExecutionRole (Stacksets の実行を許可するための IAM ロール)を作成します。	利用者																		
2	AWS Configログ保存用 S3 バケット構築	AWS の設定履歴、設定スナップショットを保存するための S3 バケットを用意します。	構築担当者																		
3	AWS Config 有効化	全リージョンの AWS Config を有効化します。	構築担当者																		
4	AWS Config アグリゲータ承認	当社監査環境との AWS Config 接続を承認します。	構築担当者																		
監査内容	本サービスのの監査内容は「【別紙】【セキュリティ監査サービス】セキュリティルール一覧」をご参照ください。 監査項目は CIS Amazon Web Servcie Foundations Benchmark、AWS セキュリティベストプラクティスに準拠した項目となっております。																				

通知内容	監査結果をメールにて通知します。通知内容は以下の通りです。	
	通知項目	通知内容
	ルール名	検知した監査ルール名を通知します
	検知対象リソース情報	検知対象リソースの情報を通知します ・AWS アカウント ・リージョン ・リソースタイプ ・リソース ID ・ARN
	検知理由	何が原因でルール違反/問題となっているかを通知します
	修正方法	修正方法に関する AWS ドキュメントのリンクを通知します
提供価格	個別相談	
留意事項	セキュリティ監査にて検出された特定ルールの違反/問題については利用状況によっては是正対応を判断頂く必要があります。	
サービス価格	個別見積となります。	
連絡方法	連絡先	お問合せポータル
	連絡方法	お問合せポータル-[その他問合せ]
	受付方法	24 時間 365 日 (システムメンテナンス時を除く)
	対応時間	平日 9:00-17:00 (土・日・祝日、年末年始を除く)