HITACHI
Inspire the Next

クラウドワークロードセキュリティサービス
トライアル簡単導入ガイド

株式会社日立ソリューションズ

CWSS_trial22-11-001

HITACHI
Inspire the Next

Contents

HITACHI
Inspire the Next

Contents

クラウドワークロードセキュリティサービスとは

HITACHI
Inspire the Next

AWS

クラウド上のバラバラに
管理された仮想リソース

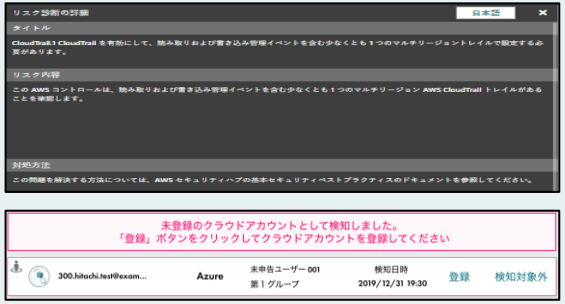
Azure

システム単位で可視化し、管理先の事業・部署・担当者がすぐ分かる

マイページ
管理対象とリスク状況がすぐ分かる

リスクのトリアージ
点検対象の優先順位がすぐ分かる

リスクの内容と対策
リスクの内容と対策がすぐ分かる



会社に未許可で利用している
クラウドアカウントの検出も可能

AWS：Amazon Web Services，Azure：Microsoft Azure　※画面内、CWSSはクラウドワークロードセキュリティサービスの略称です

クラウドワークロードセキュリティサービスの主要機能

HITACHI
Inspire the Next

全数把握

シャドーアカウント検知

・CWSSに登録していないクラウドアカウントを自動的に検知、登録を促進。

・登録後は、クラウドアカウントに紐づくリソース情報を自動収集。

資産管理

・クラウド上のリソースをシステム単位で管理。

・リソースに関する資産情報（リージョン、OSなど）を自動的に収集し、ユーザーが管理したいメタ情報を任意に定義して管理可能。

常態監視

リスクの一元管理

・AWS CIS（*1）、Azure CIS（*2）といった業界標準のリスク検知に対応。

・自動でチェックする項目をユーザーが任意で指定可能なため、不要な検知項目を排除し、ユーザーの負荷を軽減。

アラート管理

・Microsoft Teamsと連携することで、リスク検知時にアラートを受け取ることが可能

・アラートの種類や通知タイミングなど柔軟に設定できるため、必要なアラートを必要なときに受け取り、万が一の際の対応遅延を防止。

（*1）CIS Amazon Web Services Foundations Benchmark，（*2）CIS Microsoft Azure Foundations Benchmark
※CWSSはクラウドワークロードセキュリティサービスの略称です

プロダクトコンセプト

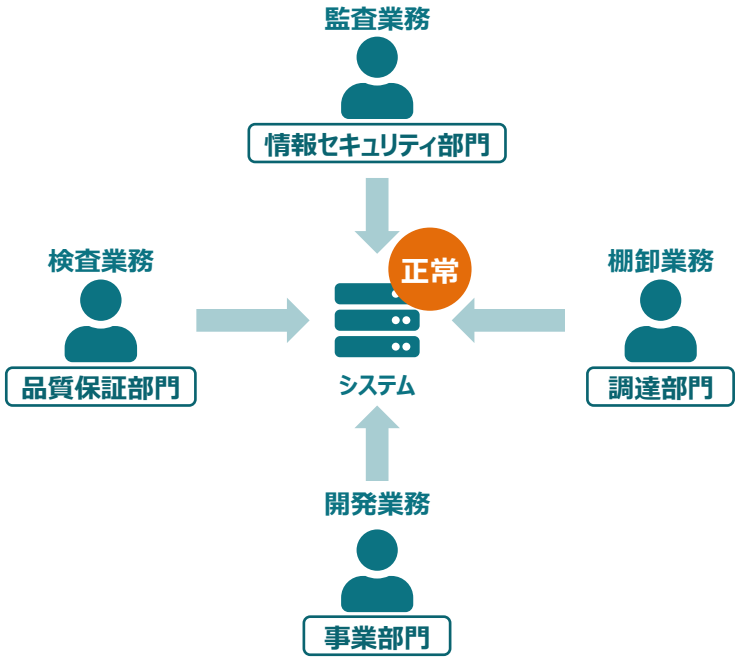
HITACHI
Inspire the Next

「資産（システム）」を管理し、「正常という安心」を可視化する

全数把握

全社のシステムを可視化
システムの関係者をつなぐ

PDCAをスムーズに循環



常態監視

システムの正常状態を監視
管理者の不在を回避

システムの常態を維持

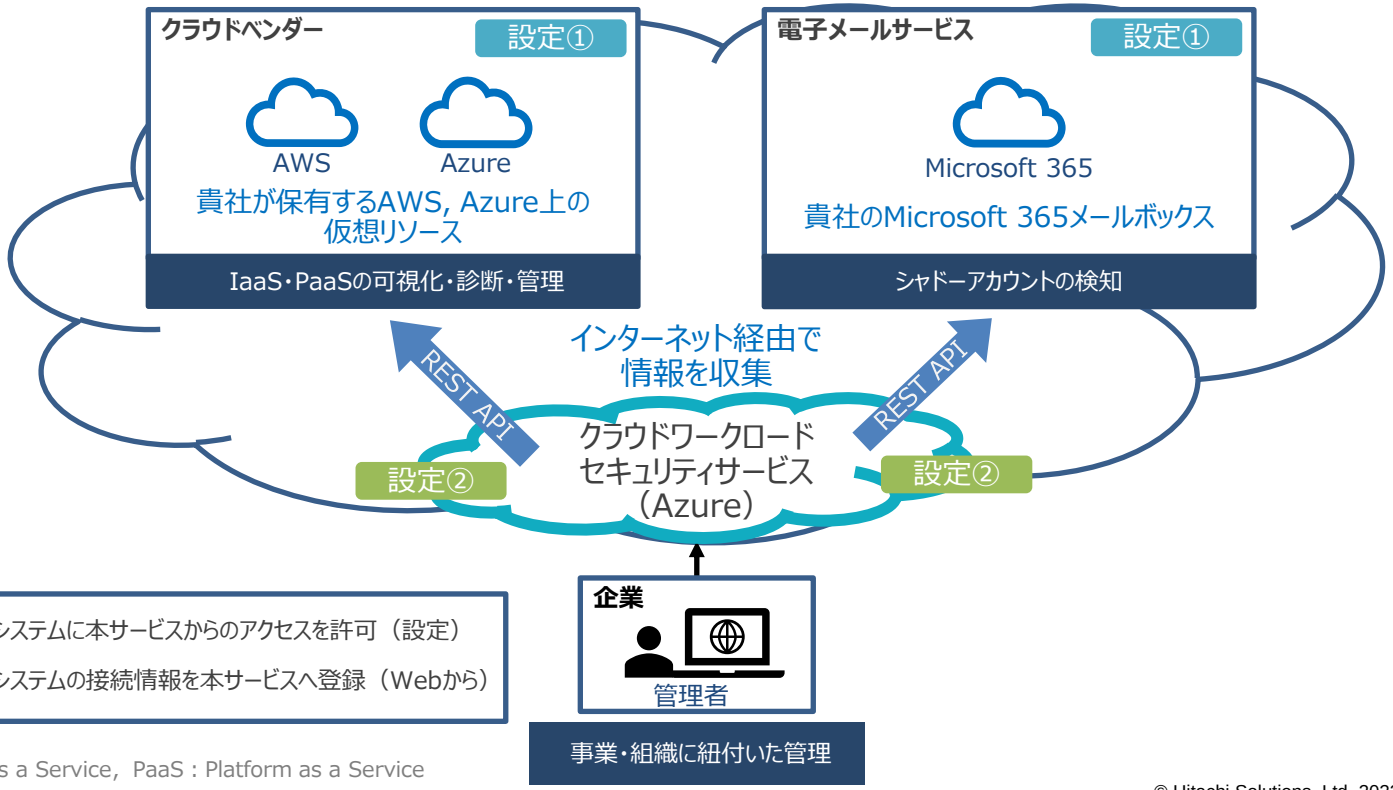
知りたいときにシステムの情報をすぐ見られる、連絡とりたいときに管理者がすぐ分かる、
企業が管理している情報とクラウドから集める情報をクラウドワークロードセキュリティサービス（以降、CWSS）がつなぎます

HITACHI
Inspire the Next

Contents

システム構成

お客様の環境でサーバー設置の必要なし
エージェントレスのため、サーバーへのインストール作業も不要



設定① ：貴社システムに本サービスからのアクセスを許可（設定）

設定② ：貴社システムの接続情報を本サービスへ登録（Webから）

IaaS：Infrastructure as a Service，PaaS：Platform as a Service

トライアルプランについて

HITACHI
Inspire the Next

概要

クラウドワークロードセキュリティサービスを

12カ月間、無料で利用になれます

制限事項

- クラウドリソースのリスクを閲覧できるのは最初に登録したクラウドアカウント５件分です
- 検知したシャドーアカウントのうち、詳細情報を閲覧できるのは最初に検知した５件です
- クラウドリソースとは、クラウドベンダが提供する以下のカテゴリに属する仮想機器です
  コンピュータ・データベース・ファイルサーバー(ストレージ)・サーバーレス・ロードバランサ・ファイアウォール・コンテナ
- サポートサービスはありません

トライアル終了時

30日以内に有償サービスをご契約いただける場合、設定などはそのまま利用可能です

動作環境

■動作環境

クラウドワークロードセキュリティサービス	
対象クラウドサービス	Amazon Web Services、Microsoft Azure
対象ブラウザー	Google Chrome
対象メールサーバー	Microsoft 365

■前提条件

	AWS	Azure
必要な権限	・Administrator Access	・Azure ADの権限として以下のどれか クラウド アプリケーション管理者 ・ アプリケーション管理者 ハイブリッド ID の管理者 ・ グローバル管理者 ・RBACの権限として以下のどれか Contributor（共同作成者）・ 所有者
前提となるサービス	・AWS Config ・AWS CloudFormation（導入時に必要） 任意（リスクを収集する場合） ・Amazon Classic Inspector ・AWS Security Hub ・AWS Systems Manager	・Azure Cloud Shell（導入時に必要） 任意（Azure CIS 1.3.0 のリスクを収集する場合） ・Microsoft Defender for Cloud（強化されたセキュリティ機能）

トライアルの流れ

HITACHI
Inspire the Next

凡例）〇：必須、－：任意

項番	手順	内容	必須	備考
1	利用申し込み	Webサイトからお申し込みください。カスタマーコード、アカウント情報などが記載された登録完了メールが送付されます。	〇	－
2	管理コンソールへのサインイン	１の手順で得た情報をもとに、本サービスの管理コンソールにサインインします。	〇	－
3	クラウドワークロードセキュリティサービスへの接続情報の登録	クラウド上のリソース情報を収集するため、貴社システムへのアクセス許可と本サービスへの接続情報の登録を行います。	〇	－
4	システム情報の登録	管理コンソールから、システムの情報を本サービスに登録します。	〇	－
5	メールシステムの接続	シャドーアカウントの検知機能を利用する場合、電子メールを検索するための権限を、本サービスに設定します。	－	シャドーアカウントの検知機能を利用しない場合、本手順は不要です。
6	アラート通知の設定	Microsoft Teamsでシステムのアラート通知を受け取るために、受け取り側（Microsoft Teams）と送り側（本サービス）の設定を行います。	－	Microsoft Teamsで通知を受け取らない場合は、本手順は不要です。

クラウドサービス上のシステムに行うこと

HITACHI
Inspire the Next

アクセス方法	REST APIでアクセス
処理内容	本サービスにクラウドアカウントを登録し、 クラウド上のリソース情報を収集します。
アクセス時間帯	0時、6時、12時、18時
データ量	リソース数に依存
取得する データの内容	AWS、Azureのポータルで参照できる情報のうち、 リソースとセキュリティに関する情報のみ

メールサーバーに行うこと

HITACHI
Inspire the Next

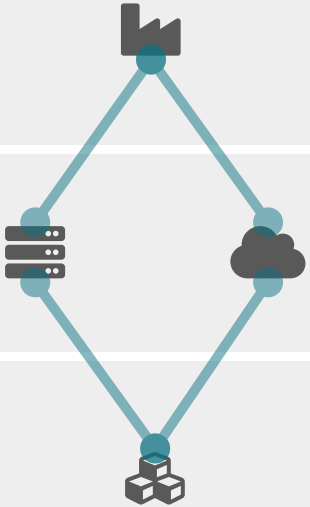
アクセス方法	REST API（Microsoft Graph）でアクセス
処理内容	メールボックスを検索し、送信元アドレスがAWSまたはAzureなどのIaaS・PaaSの通知用アドレスであるメールの情報を取得
アクセス時間帯	深夜01:00～03:00　（※アクセス時間帯は現バージョンでは変更不可）
取得するデータの内容	●送信元メールアドレス　●受信日時 ●受信先メールアドレス　●件名　※本文は取得しません
アクセス範囲	貴社メールボックスのみ

HITACHI
Inspire the Next

Contents

アセットについて

■アセットとは



上位アセット

事業情報

複数のシステム情報とクラウドアカウント情報をグルーピングして
管理する情報の単位。
主に事業企画・事業部門の部長などを想定した管理形態。

システム・クラウドアカウント情報

複数のリソース情報をグルーピングして管理する情報の単位。
システム情報は、主にシステム管理者向けの管理形態。
クラウドアカウント情報は、主にアカウント発行者向けの管理形態。

リソース情報

CWSSで管理する情報の最小単位。
リソース情報は、VMやRDBなどクラウド上にあるリソース、
またはオンプレミス上のVM、ロードバランサなどの機器情報の管理形態。

下位アセット

■各アセットの関係

原則として、事業情報→システム・クラウドアカウント情報→リソース情報と、
上から下に管理者の権限などのさまざまな設定項目が継承されていく。
権限の力関係も**事業 ＞ システム＝クラウドアカウント ＞ リソースの順**となる。

RDB：Relational Database
※CWSSはクラウドワークロードセキュリティサービスの略称です

アセットの情報形態

■アセットのカード情報と詳細情報

アセットの情報は、主に以下の2つの情報形態で表現される。
① アセットのサマリーを表す「**検索情報**」。
② アセットの詳細な中身を参照することができる「**管理情報**」。

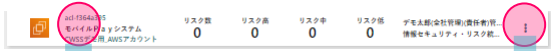
検索情報

事業カード

システムカード

クラウドアカウントカード

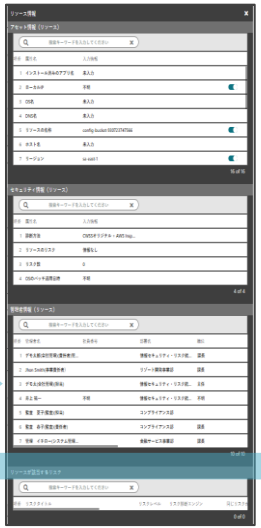
リソースカード



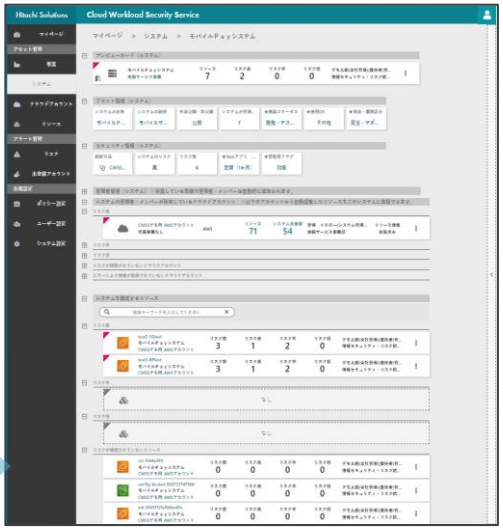
検索情報から権限のあるアセットには
管理情報を参照することができる

管理情報

アセットの全情報表示



アセットの簡易情報表示

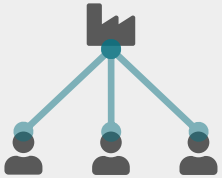


アセットの管理者・メンバー

HITACHI
Inspire the Next

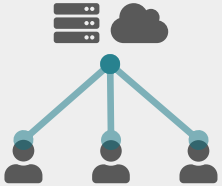
■アセットの管理者・メンバー

各アセットには管理者とメンバーを設定できます。
管理者は対象アセットの編集など全ての操作が可能ですが、**メンバーは参照のみ**となります。



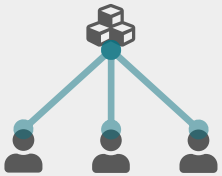
事業の管理者・メンバー

事業情報にアクセスできるユーザー。
事業情報に紐づけているシステム・クラウドアカウント、さらにその下に紐づいている
リソースの詳細情報にアクセス可能。



システム、クラウドアカウントの管理者・メンバー

システム、クラウドアカウント情報にアクセスできるユーザー。
事業情報に紐づけているシステム・クラウドアカウント、さらにその下に紐づいている
リソースの詳細情報にアクセス可能。



リソースの管理者・メンバー

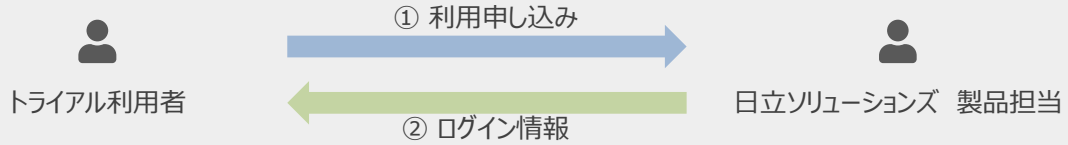
リソース情報にアクセスできるユーザー。

HITACHI
Inspire the Next

Contents

【手順１】トライアルの利用申し込み

#	手順	内容
1	利用申し込み	Webサイトからお申し込みください。カスタマーコード、アカウント情報などが記載された登録完了メールが送付されます。



①以下のURLからお申込みください。
https://www.hitachi-solutions.co.jp/cloud_orchestrator/lp/

②製品担当窓口よりメールで以下の内容を返信します。

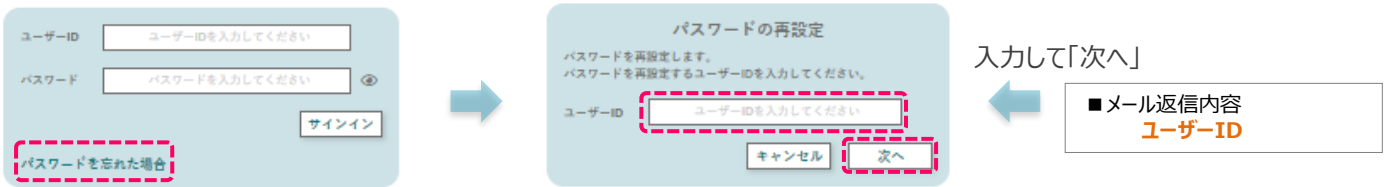
【メール内容】
・管理コンソールのURL
・カスタマーコード
・ユーザーID

【手順２】管理コンソールへのサインイン

#	手順	内容
2	管理コンソールへのサインイン	１．の手順で得た情報をもとに、クラウドワークロードセキュリティサービスの管理コンソールにサインインします。

①メールに記載された管理コンソールのURLにアクセスします。

②【パスワードを忘れた場合】をクリックし、メールに記載された「ユーザーID」を入力して【次へ】をクリックします。

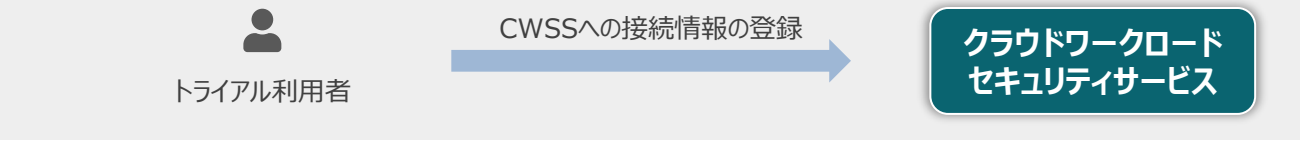


③パスワード再設定の手順を記載したメールが送信されます。メールに記載されているURLからパスワードを設定してください。

④管理コンソールURLにアクセスし、「ユーザID」と③で設定した「パスワード」を入力し、サインインします。

【手順３】クラウドワークロードセキュリティサービスへの接続情報の登録①

#	手順	内容
3	CWSSへの接続情報の登録	クラウド上のリソース情報を収集するため、お客様所有のシステムへのアクセス許可と、本サービスへの接続情報の登録を行います。



■マイページ

CWSSへサインインすると、**マイページ**と呼ばれるページに遷移します。
ここでは、**サインインしたユーザーが管理している事業**、システム、クラウドアカウント、リソースの**各アセットが表示**されます。

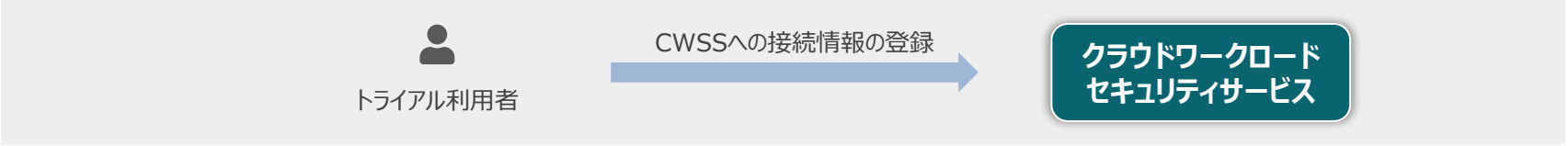
セキュリティ監査など、リスクのチェックをする際は
このページにあるシステム、リソースをクリックして詳細な情報を閲覧してください。

なお、初回ログイン時もこのページから各アセットを登録することができます。

※CWSSはクラウドワークロードセキュリティサービスの略称です

【手順３】クラウドワークロードセキュリティサービスへの接続情報の登録②

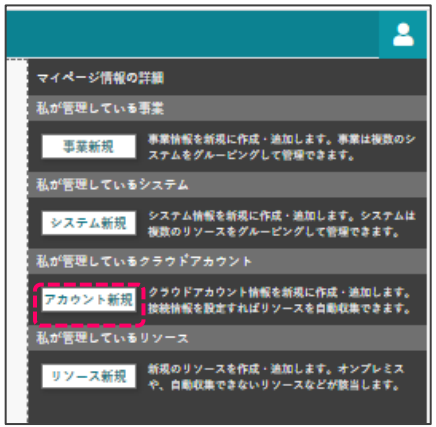
#	手順	内容
3	CWSSへの接続情報の登録	クラウド上のリソース情報を収集するため、お客様所有のシステムへのアクセス許可と、本サービスへの接続情報の登録を行います。



■マイページ

画面右上の「＜」をクリックして、設定変更画面を表示します。
（赤い点線で囲っている部分となります。）

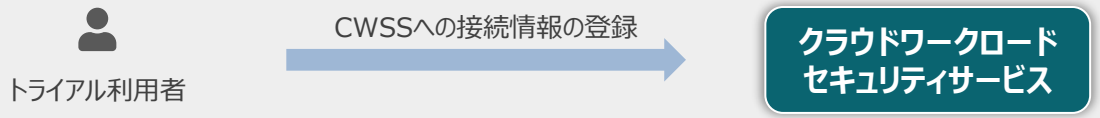
表示される設定変更画面より、
「アカウント新規」ボタンをクリックします。



※CWSSはクラウドワークロードセキュリティサービスの略称です

【手順３】クラウドワークロードセキュリティサービスへの接続情報の登録③

#	手順	内容
3	CWSSへの接続情報の登録	クラウド上のリソース情報を収集するため、お客様所有のシステムへのアクセス許可と、本サービスへの接続情報の登録を行います。



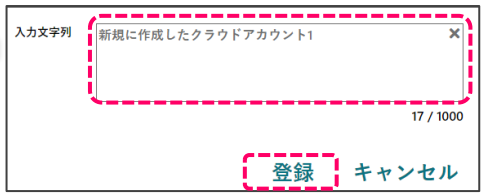
■新規に作成したクラウドアカウント情報

■クラウドアカウント情報

ここでは管理するクラウドアカウントに関する情報を登録するページになります。

「アカウントの名称」をクリックするとダイアログが開きます。
クラウドアカウントの利用目的を入力してください。
（例） XXサービス開発環境

入力後、「登録」をクリックしてください。

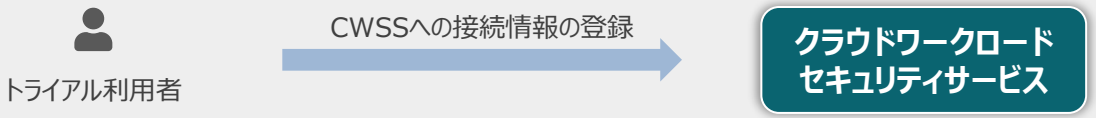


「アカウントの説明」の入力は任意となります。

※CWSSはクラウドワークロードセキュリティサービスの略称です

【手順３】クラウドワークロードセキュリティサービスへの接続情報の登録④

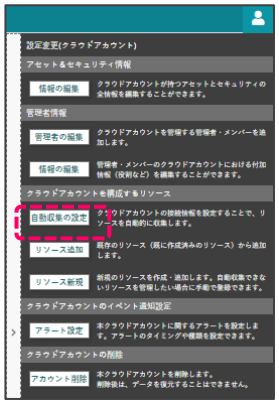
#	手順	内容
3	CWSSへの接続情報の登録	クラウド上のリソース情報を収集するため、お客様所有のシステムへのアクセス許可と、本サービスへの接続情報の登録を行います。



■新規に作成したクラウドアカウント情報

画面右上の「＜」をクリックして、設定変更画面を表示します。
（赤い点線で囲っている部分となります。）

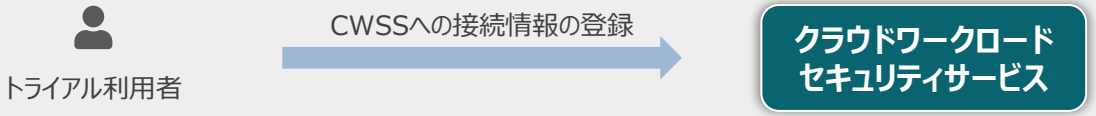
表示される設定変更画面より、
「自動収集の設定」ボタンをクリックします。



※CWSSはクラウドワークロードセキュリティサービスの略称です

【手順３】クラウドワークロードセキュリティサービスへの接続情報の登録⑤

#	手順	内容
3	CWSSへの接続情報の登録	クラウド上のリソース情報を収集するため、お客様所有のシステムへのアクセス許可と、本サービスへの接続情報の登録を行います。

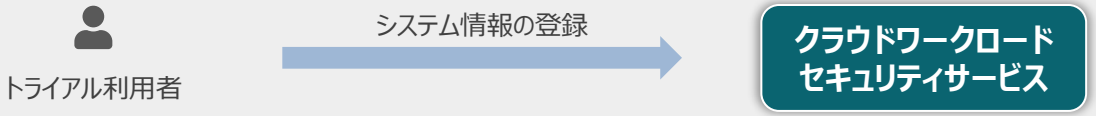


接続するクラウドアカウントの種類によってリソースの自動収集の設定手順が異なります。
接続するクラウドアカウントの種類に合わせ、画面上部のタブより、AWS、Azureを選択します。
以降、画面に表示された手順に従って、リソースの自動収集の設定を行います。画面に表示された手順の詳細については、**本スライドのP.44～P.49**を参照してください。

※CWSSはクラウドワークロードセキュリティサービスの略称です

【手順４】システム情報の登録①

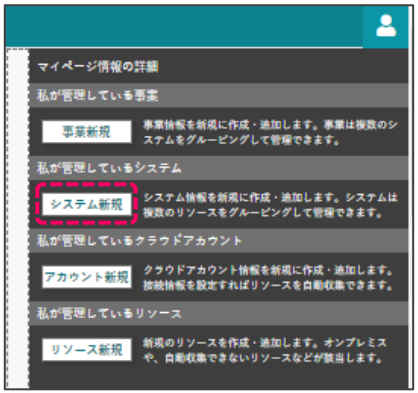
#	手順	内容
4	システム情報の登録	管理コンソールから、システムの情報をCWSSに登録します。



■マイページ

画面右上の「＜」をクリックして、設定変更画面を表示します。
（赤い点線で囲っている部分となります。）

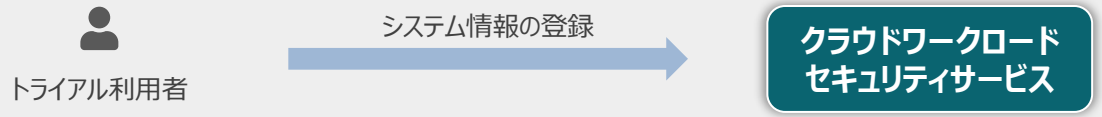
「システム新規」ボタンをクリックします。



※CWSSはクラウドワークロードセキュリティサービスの略称です

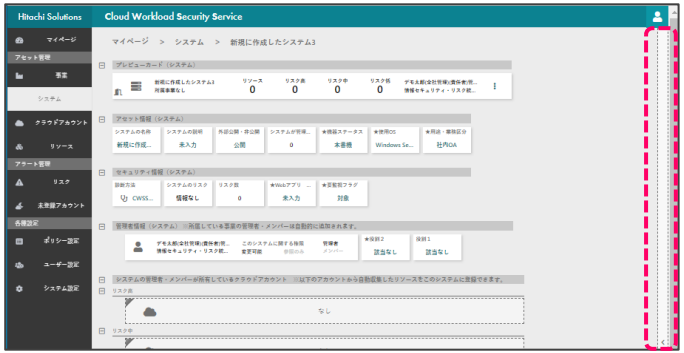
【手順４】システム情報の登録②

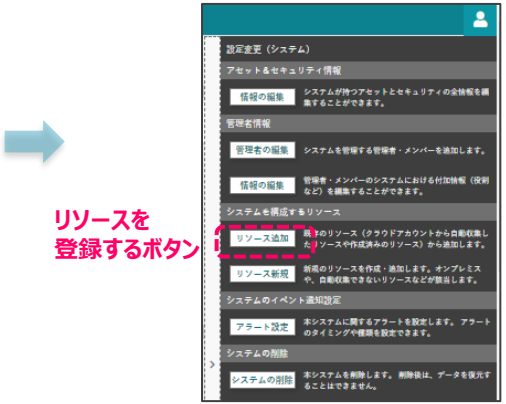
#	手順	内容
4	システム情報の登録	管理コンソールから、システムの情報をCWSSに登録します。



■新規に作成したシステム情報

ここでは管理したシステムに関する情報を登録するページになります。
自分で入力する項目もありますが、自動で値が入る項目もあります。
このページでまず初めにすることは、この**システムを構成する「リソースの登録」**からです。
リソースは手順＃３で登録した**クラウドアカウントの接続情報から自動収集**したリソースから選択することができます。





説明は次スライドに続きます

※CWSSはクラウドワークロードセキュリティサービスの略称です

【手順４】システム情報の登録③

#	手順	内容
4	システム情報の登録	管理コンソールから、システムの情報をCWSSに登録します。

追加したいカードをクリックするとカードがアクティブになります。
「すべて選択」をクリックすると、選択可能なカードがすべてアクティブになります。

※複数のクラウドアカウントを登録した場合で、登録するシステムを
分けたい場合は「すべてを選択」を押さず、個別に選択をお願いいたします。

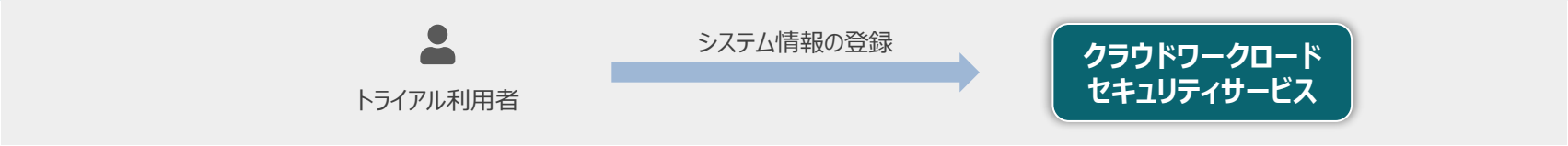
カードの選択が終わったら、
ダイアログ上部の「適用」を
クリックします。

これでリソースの追加は
完了です。

※CWSSはクラウドワークロードセキュリティサービスの略称です

【手順４】システム情報の登録④

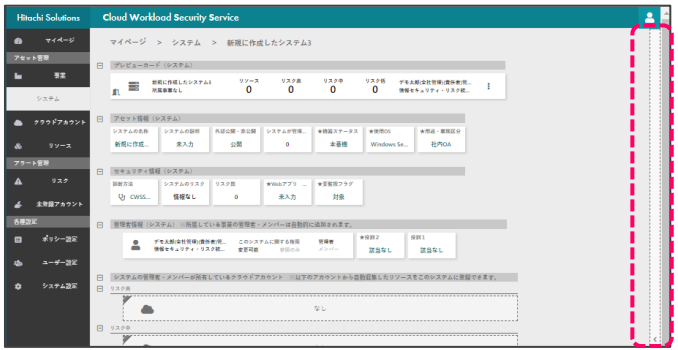
#	手順	内容
4	システム情報の登録	管理コンソールから、システムの情報をCWSSに登録します。



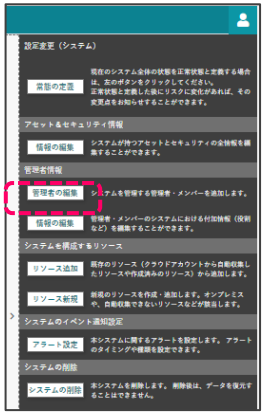
■新規に作成したシステム情報

システムに管理者を追加することで、システム情報に対する読み取りまたは書き込みを許可することができます。

システムに対する読み取りまたは書き込みを許可すると、**システムを構成するリソースにも同じ権限が自動で継承**されます。



管理者を
登録するボタン

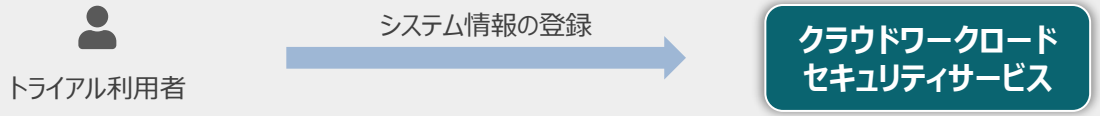


管理者の追加の手順は、
リソースの追加とほぼ同じです。

※CWSSはクラウドワークロードセキュリティサービスの略称です

【手順４】システム情報の登録⑤

#	手順	内容
4	システム情報の登録	管理コンソールから、システムの情報をCWSSに登録します。

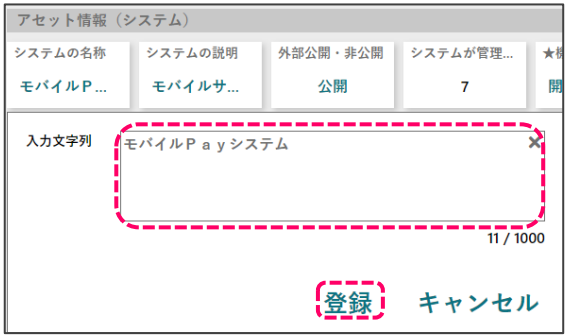


■新規に作成したシステム情報

システムの名称を設定できます。

名称をクリックするとダイアログが開きます。

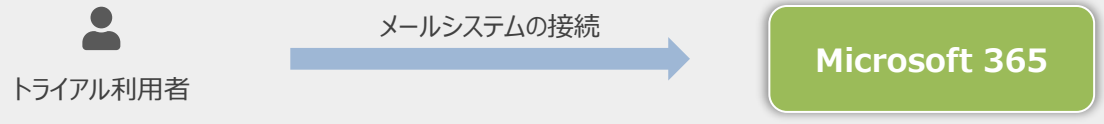
システム名を入力し、「登録」をクリックしてください。



※CWSSはクラウドワークロードセキュリティサービスの略称です

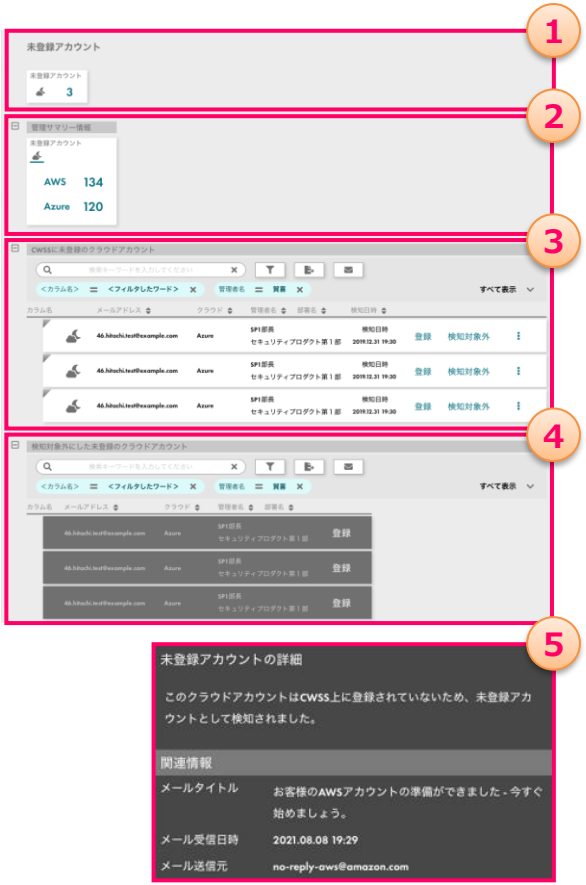
【手順５】メールシステムの接続①

#	手順	内容
5	メールシステムの接続	シャドーアカウントの検知機能を利用する場合、電子メールを検索するための権限を本サービスに設定します。



以降、画面に表示された手順に従って、リソースの自動収集の設定を行います。画面に表示された手順の詳細については、**本スライドのP.50～P.51**を参照してください。

【手順５】メールシステムの接続②



1．ヘッダ情報
未登録アカウントの全数を表示します。

2．管理サマリー情報
未登録アカウントの内訳を表示します。
現在は、AWS、Azureの件数を表示します。

3．クラウドワークロードセキュリティサービスに未登録のクラウドアカウント
CWSSが検知した未登録のクラウドアカウントのリストを表示します。

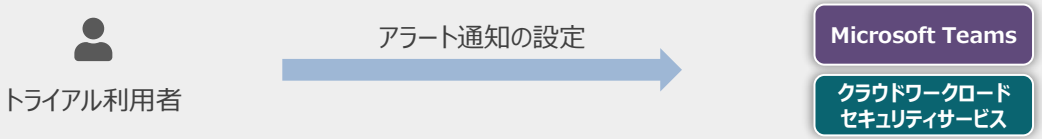
4．検知対象外にした未登録のクラウドアカウント
3. で検知対象外にした未登録アカウントリストの一覧を表示します。
なお、間違えてボタンを押してしまったことに備えて、本リストにあるものは再登録できます。

5．未登録アカウントの詳細
未登録アカウントカードの３点リーダー（右端）から、対象の未登録アカウントの詳細を閲覧することができます。
関連情報には以下の３つの情報を表示します。
①メールタイトル
②メール受信日時
③メール送信元

※CWSSはクラウドワークロードセキュリティサービスの略称です

【手順６】アラート通知の設定手順①

#	手順	内容
6	アラート通知の設定	Microsoft Teamsでシステムのアラート通知を受け取るために、受け取り側（Microsoft Teams）と送り側（本サービス）の設定を行います。



■受け取り側（Microsoft Teams）の設定

・Teamsのチャネル作成
・作成したチャネルにアラートを見る人を追加する

Microsoft Teams

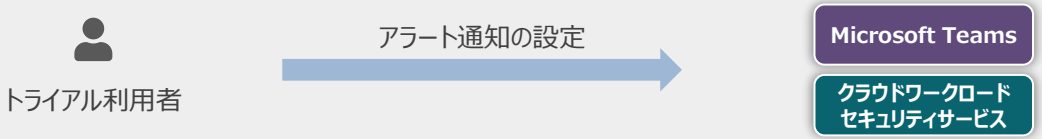
■送り側（クラウドワークロードセキュリティサービス）の設定

・作成したTeamsのチャネルのリンク先（※1）を取得。
・取得したリンク先をクラウドワークロードセキュリティサービスに設定。

※1 作成したTeamsのチャネルのリンク先（Webhook URL）の取得手順の詳細は以下のURLを参照。
https://docs.microsoft.com/ja-jp/microsoftteams/platform/webhooks-and-connectors/how-to/add-incoming-webhook

【手順６】アラート通知の設定手順②

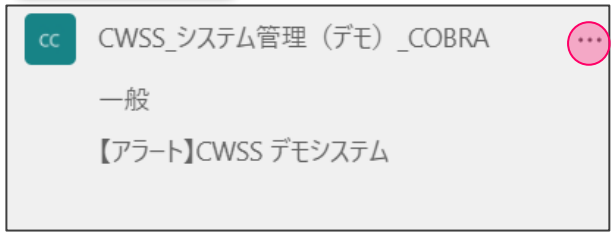
#	手順	内容
6	アラート通知の設定	Microsoft Teamsでシステムのアラート通知を受け取るために、受け取り側（Microsoft Teams）と送り側（本サービス）の設定を行います。



システムの管理者・メンバーは、以下の設定手順を実施すると自分が管理しているシステムのアラート通知を受け取れます。

STEP１：アラート受け取るためのTeamsのチャネルを作成します。

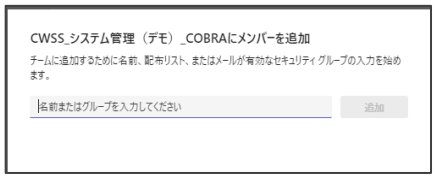
Microsoft Teams　システム管理者・メンバー



①アラートを受け取るためのチームを作成します。
　例：「CWSS_システム管理（デモ）__COBRA」
②その中に以下のチャネルを作成します。
　・【アラート】CWSSデモシステム

STEP２：アラートを受け取る人を作成したチャネルに追加します。

Microsoft Teams　システム管理者・メンバー

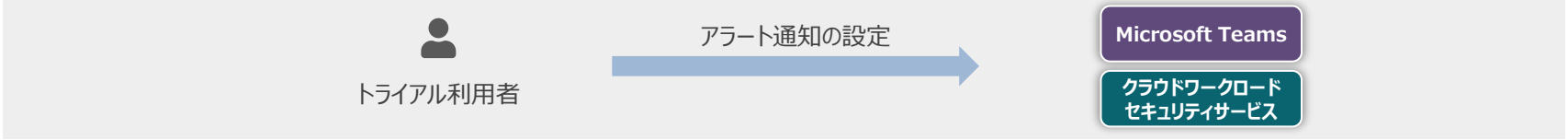


①CWSSのアラートを見せたい人を本チームに所有者、または
　メンバーとして追加します。

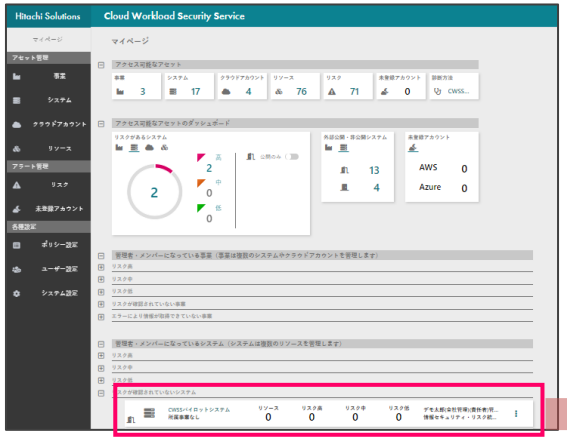
※CWSSはクラウドワークロードセキュリティサービスの略称です

【手順６】アラート通知の設定手順③

#	手順	内容
6	アラート通知の設定	Microsoft Teamsでシステムのアラート通知を受け取るために、受け取り側（Microsoft Teams）と送り側（本サービス）の設定を行います。

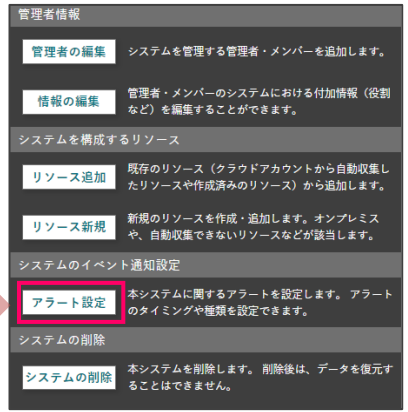


STEP１：トップ画面（マイページ）から自分が管理しているシステムをクリックします。



STEP２：システム画面の右端にあるブレードメニューバーをクリックします。

STEP３：「アラート設定」ボタンをクリックします。



【手順６】アラート通知の設定手順④

HITACHI
Inspire the Next

STEP4： アラート設定画面にて以下の手順を実施します。

アラートの通知の設定例

定期発報：ON　毎週月曜日
リスクレベルでの発報可否：全てチェック（リスク高・リスク中・リスク低）

※CWSSはクラウドワークロードセキュリティサービスの略称です

1．設定適用ボタン
アラート通知設定で反映した設定を「適用」「キャンセル」することができます。
アラート一時的に止めたい場合は「アラート一時停止」で止めることもできます。

2．アラート通知の設定
システムのアラートを通知するための通知先（通知方法）、タイミング・頻度、発報内容を設定します。具体的には以下になります。

①アラートの通知方法
アラートの通知方法を指定します。
現在のバージョンでは**Microsoft Teamsのみ**です。

②アラートのタイミング
アラートのタイミングを設定します。
＜即時発報をオンにした場合＞
・リスクを検知した場合に発報します。
現在、CWSSではリスク検知は１日以下の４時刻となります。
00:00、06:00、12:00、18:00

＜定期発報をオンにした場合＞
・発報対象のリスクイベントを定期的に発報します。
定期間隔の指定は以下の中から選べます。
毎日（時間指定）、毎週（曜日指定）、毎月（日付指定）
なお、毎週と毎月の時間は 6:00で固定です。

③リスクレベルでの発報可否
発報するリスクイベントのうち、発報するリスクレベルを指定できます。リスクレベルは以下の３つ。
・リスク高、リスク中、リスク低

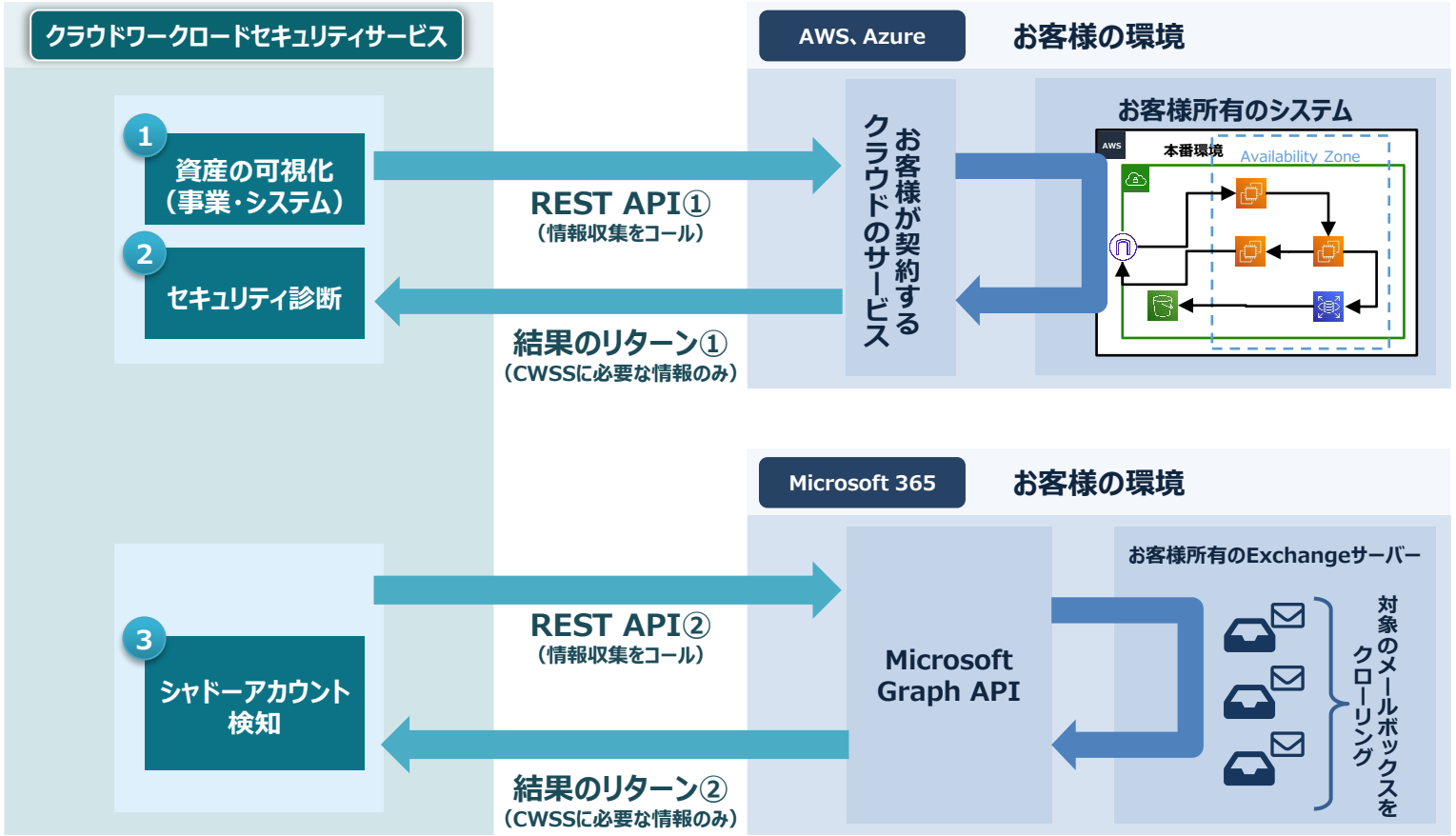
3．アラートをCWSSから送るための設定手順
アラートを受け取るための設定の手順になります。
表記にある設定手順を実施してください。

【手順６】アラート通知の設定手順⑤

リスクが存在する場合、リスク低　リスク中　リスク高　ごとに通知されます。

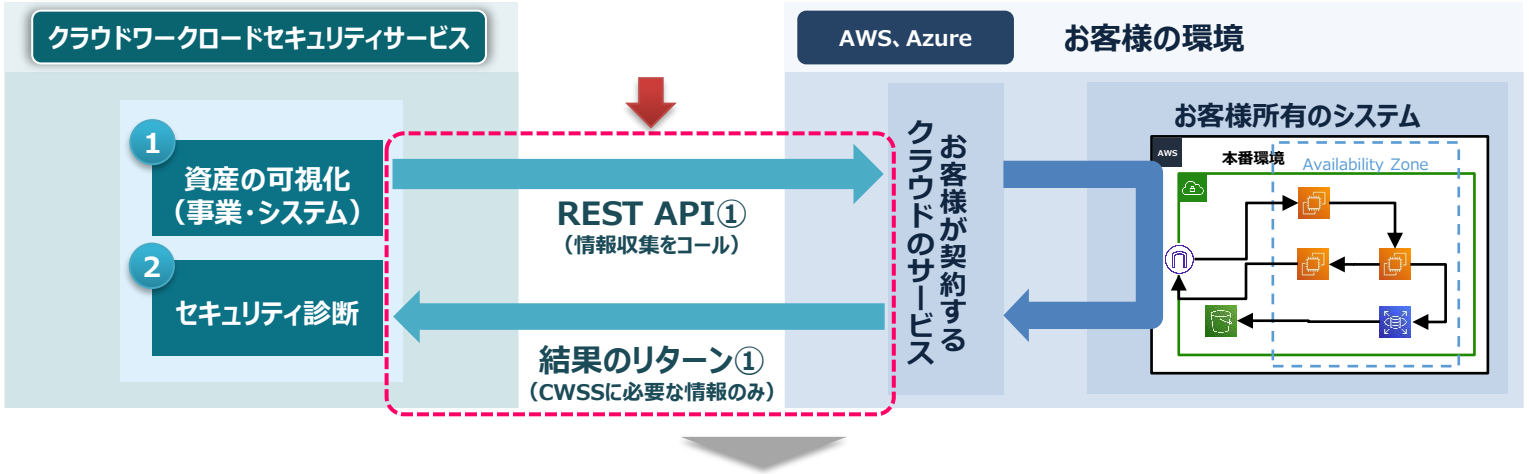
※画像内、CWSSはクラウドワークロードセキュリティサービスの略称です

お客様環境における影響　～システムの全体像～



※CWSSはクラウドワークロードセキュリティサービスの略称です

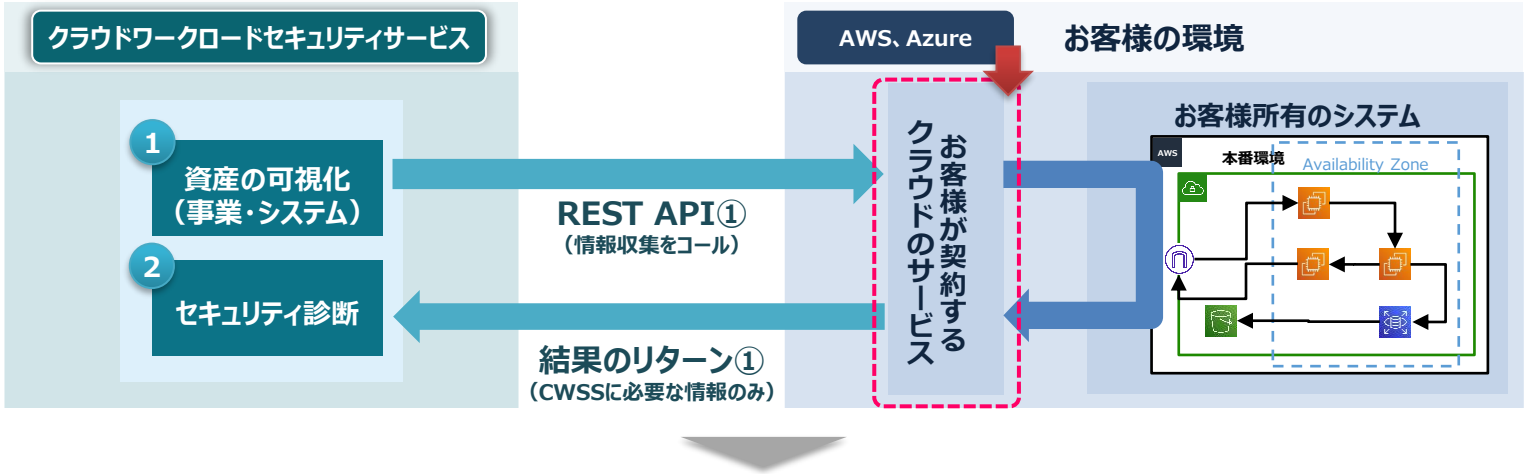
お客様環境における影響 ～お客様所有のシステムへの影響①～



REST APIをコールする際のお客様環境における影響

1	アクセス方法	CWSSがお客様が契約済みのクラウドサービス（クラウド間通信）。
2	処理内容	本サービスにクラウドアカウントを登録し、クラウド上のリソース情報を収集します。
3	アクセス時間帯	00:00、06:00、12:00、18:00（UTC+9）
4	アクセス頻度	4回/日（リトライは3回）
5	データ量	クラウド間通信のため、お客様所有のシステムには影響はない。 （プリンシパルを分けていれば、CWSS専用のREST APIとしてコールするため影響なし）
6	取得する情報の内容	AWS、Azureのポータルで参照できる情報のうち、リソースとセキュリティに関する情報のみ。

お客様環境における影響 ～お客様が契約するサービス～



お客様が契約するサービス（事前に用意して欲しいサービス）

1	AWS	AWS Inspector（7.2米ドル※）	お客様所有のシステムに対して、CWSSがネットワーク到達可能性、およびホスト評価をする際に利用します。 これにより、インターネット経由でポートベースやVPC ピアリング接続、VPNを通じて該当EC2にアクセスされる可能性があるかどうかを評価、またAWS EC2の脆弱性を評価できます。
2		AWS Security Hub（4.8米ドル※）	お客様所有のシステムに対して、CWSSが「CIS AWS Foundations Benchmark」の評価基準で評価する際に利用します。
3		AWS CloudFormation（無料※）	お客様所有のシステムに対して、CWSSがアクセスするためのIAMユーザーアカウントをプロビジョニングする際に利用します。
4		AWS Config（2.8米ドル※）	お客様所有のシステムに対して、CWSSが各リソースの情報を収集する際に利用します。
5	Azure	Security Center（無料）	お客様所有のシステムに対して、CWSSが各リソースの情報、および「CIS Microsoft Azure Foundations Benchmark」の評価基準で評価する際に利用します。

※ 料金は月額の参考値です。CWSSの開発チームが持つ検証環境（約100リソース、10VM）のコストを算出した結果になります。

※CWSSはクラウドワークロードセキュリティサービスの略称です

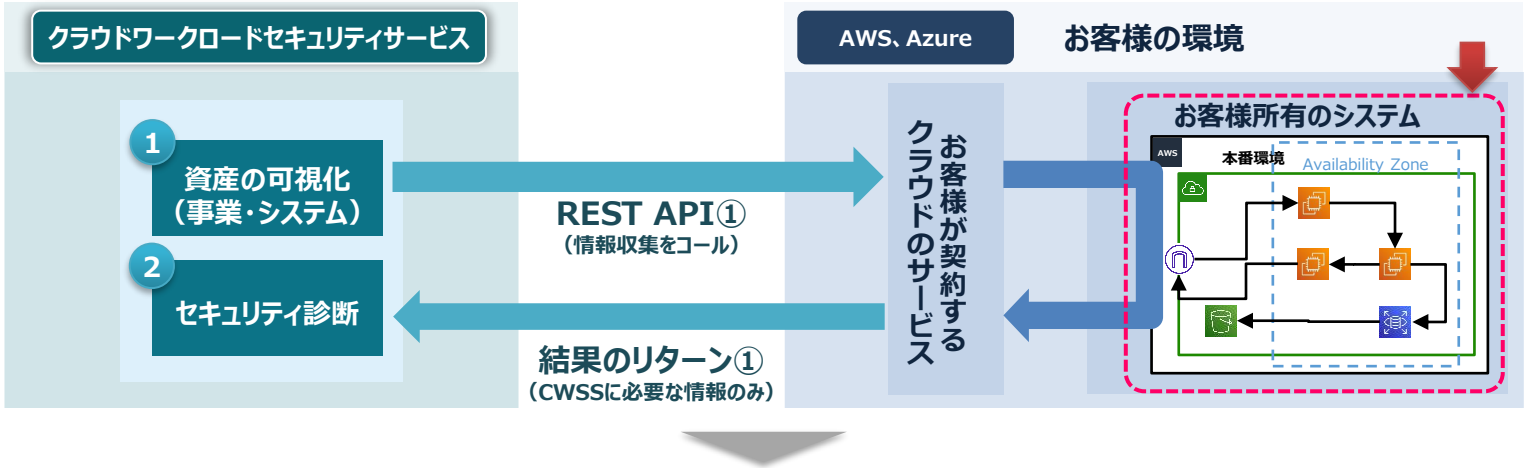
【補足】事前準備

HITACHI
Inspire the Next

クラウドワークロードセキュリティサービスが利用するサービスを動作させるための事前準備（前提条件）

1	AWS	AWS Inspector	詳細は以下のURLを参照しください。 https://docs.aws.amazon.com/ja_jp/inspector/latest/userguide/inspector_getting-started.html 以下、一部抜粋です。 以下の前提条件のタスクを実行します。Amazon Inspector の評価を実行するには、これらのタスクを完了する必要があります。少なくとも 1 つの Amazon EC2 インスタンスを実行している必要があります。AWS環境を使用して、Amazon Inspector 評価を実行します。EC2 インスタンスの起動の詳細については、「Amazon Elastic Compute Cloud のドキュメント」を参照してください。ほとんどの場合、Amazon Inspector エージェントは、評価ターゲットの各 EC2 インスタンスで実行されている必要があります。エージェントをインストールする方法の詳細については、「Amazon Inspector エージェントのインストール」を参照してください。または、Systems Manager の実行コマンドをクリックして、Amazon EC2 インスタンスにエージェントをインストールします。Amazon Inspector エージェントの詳細については、「Amazon Inspector エージェント」を参照してください。
2		AWS Security Hub	初めて AWS Security Hub コンソールを開いたときに、[開始] を選択し、次に [有効にする] をクリックします。詳細な手順は以下のURLを参照してください。 https://docs.aws.amazon.com/ja_jp/securityhub/latest/userguide/securityhub-setup-prereqs.html AWS Security Hub は、サービスがリンクされたロールを使用します。このロールには AWS Security Hub が必要とするアクセス許可と信頼ポリシーが含まれており、結果を検出して集約し、セキュリティチェックの実行に必要な前提条件となる AWS Config インフラストラクチャを設定します。AWS Security Hub がアカウントでセキュリティチェックを実行するには、そのアカウントで AWS Config レコーダーが有効になっている必要があります。
3		AWS CloudFormation	特段、事前に準備することはありません。 Administrator権限を持つIAMアカウントでクラウドアカウントの接続手順を実施ください。
4		AWS Config	特段、事前に準備することはありません。 Administrator権限を持つIAMアカウントでクラウドアカウントの接続手順を実施ください。
5	Azure	Security Center （無料）	特段、事前に準備することはありません（Security Center（無償版）はデフォルト有効）。 共同作成者、または所有者のロールを割り当てているアカウントでクラウドアカウントの接続手順を実施ください。

お客様環境における影響 ～お客様所有のシステムへの影響②～



お客様所有のシステムに追加する設定内容

1	AWS	AWS IAM	CWSSが各リソースの情報収集・リスク検知をするため、IAMアカウントの作成、各種サービスを有効化します。 ・お客様所有のシステムにアクセスするためのIAMアカウントを作成。 ・お客様所有のシステムの各リソース情報を収集するためにAWS Configを有効化。 ・お客様所有のシステムの各リソースリスクを検知するためにAWS Inspector / Security Hub を有効化。
2		AWS Config	
3		AWS Inspector	
4		AWS Security Hub	
5		AWS CloudTrail	CWSSがお客様所有のシステムにアクセスするにあたり、AWS CloudTrailのログが出力されます。
6	Azure	アプリの登録	CWSSが各リソースの情報収集・リスク検知をするため、お客様所有のシステムに「アプリの登録」をします。
7		PowerShell	PowerShellコマンドを実行できる環境を準備します。
8		Azure Monitor Logs	CWSSがお客様所有のシステムにアクセスするにあたり、Azure Monitor Logsのログが出力されます。

※CWSSはクラウドワークロードセキュリティサービスの略称です

【補足】AWS Inspectorがシステムに及ぼす影響について

HITACHI
Inspire the Next

AWS Inspectorがシステムに及ぼす影響

1	AWS	AWS Inspector	評価の実行に伴うインスタンスへの負荷については、ワークロードやお客様の環境に依存するため、 一概に説明することが困難なため、現時点ではご提供できる情報はありません。 過去事例では、t2.small のインスタンスサイズに対してルールパッケージ 4 種全てを実行 （所要時間 1 Hour） した際、 実行開始時、直ぐに多少のCPU使用率の上昇は見られたものの、その後は使用率は低い状態を推移しており、目立った CPU・ メモリーの使用率の上昇は見受けられなかったという報告があります。 CPUやメモリーに対し、スパイクするような負荷が生じたという事例は確認できておりません。 インスタンスへの負荷をご懸念されるようでございましたら、AMI などを使用しクローン環境を作成いただき、実際にかかる負荷のご確認 をご検討ください。

HITACHI
Inspire the Next

Contents

【補足】お客様所有のシステムに追加する設定内容の詳細①～AWS～

HITACHI
Inspire the Next

＃１　AWS CloudFormationのテンプレートファイルをダウンロードします。

CWSSがお客様のAWSにアクセスするためのIAMアカウントを、対象のクラウドアカウント内に作成するためのAWS CloudFormationのテンプレートファイルを以下からダウンロードしてください。

テンプレートファイルのダウンロードはここをクリック

＃２　AWS CloudFormationでスタックを作成します

＃１でダウンロードしたテンプレートファイルを使ってAWS CloudFormationでスタックを作成することで、CWSSがお客様のAWSにアクセスするためのIAMアカウントを作成します。

手順１　AWSマネジメントコンソール（スタックの作成画面）を表示します。

スタックの作成画面への移動はここをクリック

手順２　以下の手順で＃１のテンプレートファイルをアップロードします。

1．「スタックの作成画面の前提条件 - テンプレートの準備」は「テンプレートの準備完了」を設定。
2．「テンプレートの設定」でテンプレートファイルのアップロードを選択。
3．「テンプレートファイルのアップロード」の「ファイルの選択」から＃１でダウンロードしたテンプレートファイルを選択します。
4．「次へ」をクリックします。

手順３　以下の手順でスタックの詳細を指定します。

1．「スタックの名前」と「パラメータ」には任意の値を入力。
　例）スタック名：CWSSStack、ExternalID：CWSSExtID
2．「次へ」をクリックします。

手順４　以下の手順でスタックオプションを設定します。

1．何も入力せず「次へ」をクリックします
　※タグの入力は任意です。入力しても問題ありません。

手順５　以下の手順でスタックを作成します。

1．レビューページの一番下段にある「AWS CloudFormation によってIAMリソースが作成される場合があることを承認します。」をチェック「オン」にします。
2．「スタックの作成」をクリックします。

用意するIAMアカウントの権限は以下になります。
- AWSElasticBeanstalkReadOnly
- AmazonEC2ReadOnlyAccess
- AWS_ConfigRole
- AmazonSSMReadOnlyAccess
- AmazonSSMMaintenanceWindowRole
- AmazonInspectorReadOnlyAccess

CWSS用のスタックを作成して、CWSSがお客様所有のシステムにアクセスするためのIAMアカウントを作成します。

※CWSSはクラウドワークロードセキュリティサービスの略称です

【補足】お客様所有のシステムに追加する設定内容の詳細①～AWS～

＃３　CWSSにクラウドアカウントの接続情報を登録します

CWSSに＃２で作成したIAMアカウントの情報を利用して、CWSSに対象のクラウドアカウントへの接続情報を登録します。

手順１　スタックの作成が完了したことを確認します。

１．AWS CloudFormationのスタックの一覧画面に移動します。

AWS CloudFormationのスタックの一覧画面への移動はここをクリック

※＃２の手順完了後、既にスタックの一覧画面に遷移している場合は、リンクはクリックせず次の手順に進んでください。

２．＃２の手順３で入力した「スタックの名前」のスタックを探し、スタック名の下段にあるステータスの状態が「CREATE_COMPLETE」になっていることを確認します。

※「CREATE_IN_PROGRESS」の場合は、しばらくお待ちください。

手順２　クラウドアカウントへの接続情報を設定します。

※CWSSからタイムアウトで強制的にログアウトされる可能性があるため、以下のRole ARNとExternalIDは、メモ帳などに一時的に保存しておくことを推奨いたします。

１．＃２の手順３で入力した「スタックの名前」のスタックの「出力」タブをクリックします。
その後、キー「RoleARN」の値をコピーし、以下のテキストボックスに入力してください。

Role ARN　RoleARNを入力してください

２．＃２の手順３で入力した「スタックの名前」のスタックの「パラメータ」タブをクリックします。
その後、キー「ExternalID」の値をコピーし、以下のテキストボックスに入力してください。

External ID　External IDを入力してください

登録したIAMアカウントの情報に関する以下の接続情報をCWSSに入力します。

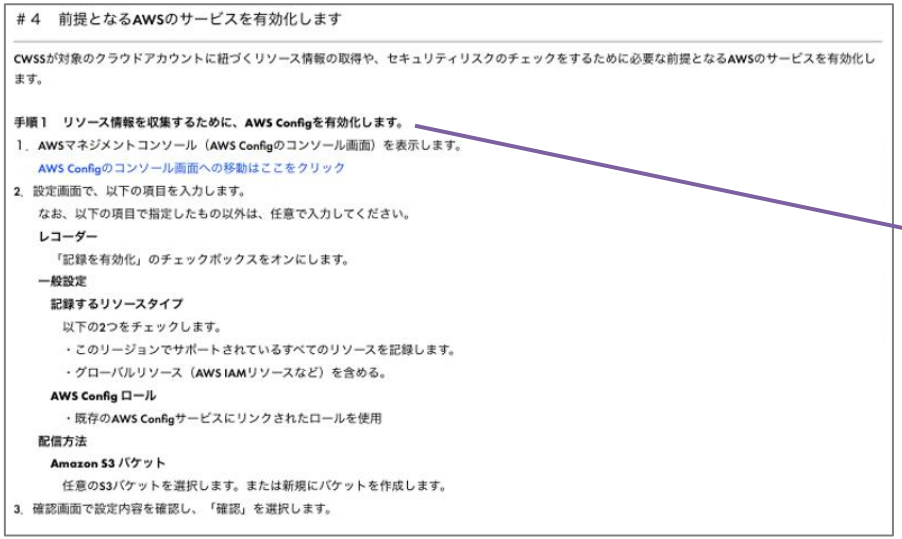
１．Role ARN
２．External ID

これにより、CWSSはクラウド上にあるお客様所有のシステムにアクセスすることができます。

※CWSSはクラウドワークロードセキュリティサービスの略称です

【補足】お客様所有のシステムに追加する設定内容の詳細①～AWS～

HITACHI
Inspire the Next



＃４　前提となるAWSのサービスを有効化します

CWSSが対象のクラウドアカウントに紐づくリソース情報の取得や、セキュリティリスクのチェックをするために必要な前提となるAWSのサービスを有効化します。

手順１　リソース情報を収集するために、AWS Configを有効化します。

1．AWSマネジメントコンソール（AWS Configのコンソール画面）を表示します。
AWS Configのコンソール画面への移動はここをクリック
2．設定画面で、以下の項目を入力します。
なお、以下の項目で指定したもの以外は、任意で入力してください。
レコーダー
「記録を有効化」のチェックボックスをオンにします。
一般設定
記録するリソースタイプ
以下の2つをチェックします。
・このリージョンでサポートされているすべてのリソースを記録します。
・グローバルリソース（AWS IAMリソースなど）を含める。
AWS Config ロール
・既存のAWS Configサービスにリンクされたロールを使用
配信方法
Amazon S3 バケット
任意のS3バケットを選択します。または新規にバケットを作成します。
3．確認画面で設定内容を確認し、「確認」を選択します。

手順２　セキュリティリスクのチェックをするために、AWS Security Hubを有効化します。
【AWS Security Hubを有効化していない場合】
1．AWSマネジメントコンソール（AWS Security Hubのコンソール画面）を表示します。
AWS Security Hubのコンソール画面への移動はここをクリック
2．AWS Security Hubを有効化するために必要な権限を設定します。
以下のURLにアクセスして設定手順を確認し、設定を実施してください。
AWS Security Hubを有効化にするために必要な権限の設定手順はここをクリック
3．AWS Security Hubを有効化します。
以下のURLにアクセスして設定手順を確認し、有効化を実施してください。
AWS Security Hubを有効化するための設定手順はここをクリック

お客様所有のシステムからリソース情報を
自動収集する際に、AWS Configの有効化が
必要になります。

レコーダー、記録するリソースタイプ、
AWS Config ロール、配信方法を設定する
必要があります。

※AWS Configのセットアップを行う際は
「今すぐ始める」をクリックする。
「1-clickセットアップ」を選択すると該当の
設定にならないため注意する。

【補足】お客様所有のシステムに追加する設定内容の詳細①～AWS～

手順3　セキュリティリスクのチェックをするために、Amazon Inspectorを有効化します。

1．AWSマネジメントコンソール（Amazon Inspectorのコンソール画面）を表示します。
　Amazon Inspectorのコンソール画面への移動はここをクリック
2．Amazon Inspectorコンソールを初めて開く場合は、「今すぐ始める」を選択します。
　そうでない場合は、ナビゲーションペインの「ダッシュボード」を選択し、
　「Help me create an Assessment」を選択します。
3．Welcome to Amazon Inspector画面で、「Network Assessments」と「Host Assessments」
　にチェックを入れます。チェックを入れたら、「Run weekly」または「Run once」を選択します。
　※「Run once」を選択した場合、一度取得したリスクの情報が自動で更新されません。
　　最新のリスク情報を取得したい場合は、Amazon Inspectorで評価を再実行してください。
4．確認画面で「OK」をクリックします。

5．ナビゲーションペインの「評価ターゲット」を選択し、新規に作成された評価ターゲット名を
　控えておきます（7．で使用します）。

6．ナビゲーションペインの「評価テンプレート」を選択し、「作成」をクリックします。
7．設定画面で、以下の項目を入力します。
　名前
　　評価テンプレートの名前を入力します。
　ターゲット名
　　5．で控えた評価ターゲット名を指定します。
　ルールパッケージ
　　診断に使用するルールパッケージを選択します。
　　※CIS Operating System Security Configuration Benchmarks-1.0は必須。
　所要時間
　　診断を実施する時間を選択します。
　　※「1時間」を推奨。
8．「作成および実行」をクリックします。

＃5　各EC2インスタンスにAWS System Managerエージェントをインストールします。

CWSSが対象となるシステムのEC2インスタンスからOSのパッチ適用状況などの情報を取得するために、
各 EC2 インスタンスに AWS Systems Manager(SSM) エージェントをインストールする必要があります。
AWS Systems Manager(SSM)エージェントは、Amazon Machine Images(AMIs)から作成したインスタンスには自動的にインストールされます。

注）インターネットにアクセスできない EC2 インスタンス（プライベートサブネットの EC2 インスタンス）は、SSM にマネージドインスタンスとして手動で登録する必要があります。

AWS Inspectorでは、
「ネットワーク到達可能性」と「ホスト評価」の
チェックをするために、以下のチェックを入れて
有効化します。

1．Network Assessments
2．Host Assessments

AWS Inspectorの評価テンプレートを作成します。
ここでのルールパッケージは、すべて選択することを
推奨としています。

AWS Inspectorの「ホスト評価」やOSの
パッチ適用状況など、EC2インスタンス内にある
情報を収集するためには、
AWS System Manager（以降、SSM）を
各EC2のインスタンスにインストールする必要があります。

なお、該当のEC2インスタンスがオンラインの場合は
自動的にインストールされますが、オフラインの場合は
手動で登録する必要があります。

【補足】お客様所有のシステムに追加する設定内容の詳細②～Azure～

Cloud Shellから、CWSSがお客様所有のシステムへ接続するための接続情報を取得します。
具体的には以下になります。

１．サブスクリプションID
２．appId
３．password
４．tenant

その際、以下のロールの権限を付与します。

・全リソースに対して読み取りの権限を付与（-role Reader）
※書き込みはできないので、リソースに対して新規作成、更新、削除はできません。
本権限ではAzure Portalから参照できるレベルのものだけが閲覧可能なので、VMの中身などの情報は見れないようになっています。
詳細は、以下をご参照ください。
（機密データを除くあらゆる種類のリソースの読み取り）
https://docs.microsoft.com/ja-jp/azure/role-based-access-control/built-in-roles#reader

CWSSがお客様所有のシステムから情報を取得するために、PowerShellを実行できる環境を準備します。その際、以下のロール権限を付与します。

・Microsoft.Compute/virtualMachines/runCommand/action
・Microsoft.Compute/virtualMachineScaleSets/virtualMachines/runCommand/action

※画像内、CWSSはクラウドワークロードセキュリティサービスの略称です

【補足】お客様所有のシステムに追加する設定内容の詳細②～Azure～

＃４　前提となるAzureのサービスを有効化します

CWSSが対象のクラウドアカウントに紐づくリソース情報の取得や、セキュリティリスクのチェックをするために必要な前提となるAzureのサービスを有効化します。

手順１　セキュリティリスクのチェックをするために、Microsoft Defender for Cloud（強化されたセキュリティ機能）を有効化します。
Microsoft Defender for Cloud（強化されたセキュリティ機能）を有効化するために以下のURLにアクセスして設定手順を確認し、設定を実施してください。
Microsoft Defender for Cloud（強化されたセキュリティ機能）を有効化にするために必要な設定手順はここをクリック

手順２　セキュリティリスクのチェックをするために、CIS Azure Foundations Benchmark を有効化します。
CIS Azure Foundations Benchmarkを有効化するために以下のURLにアクセスして設定手順を確認し、設定を実施してください。
CIS Azure Foundations Benchmarkを有効化にするために必要な設定手順はここをクリック

Azure CIS 1.3.0 のリスクを収集する場合にこの#4を実施します。

※画像内、CWSSはクラウドワークロードセキュリティサービスの略称です

【補足】お客様所有のシステムに追加する設定内容の詳細③～Microsoft 365～

HITACHI
Inspire the Next

＃１　未登録アカウント（シャドーアカウント）の検知対象となるメールサーバー側（Microsoft 365側）の設定をします。

未登録アカウント（シャドーアカウント）の検知は、ユーザーがAWSやAzureなどから送付されているメール（アカウント作成や請求など）を
探索することで、CWSSに未登録なクラウドアカウントを検知する機能です。
本手順では、ユーザーが利用しているメールサーバー（Microsoft 365）に対して、CWSSがアクセスするために必要な設定を実施します。

手順１　Microsoft 365のAzure Active Directoryにアプリケーション（CWSS）を登録します。

1．Azure Portalに、Microsoft 365の管理者アカウントでサインインします。
2．[Azure Active Directory] － [アプリの登録] － [新規登録] を選択します。
3．[アプリケーションの登録]画面で、必要な項目を入力します。入力が終わったら、[登録]を選択します。
　名前
　　本サービスのアプリケーションであることがわかるよう、アプリケーション名を入力します。
　　例）CWSS（未登録アカウント検知用）
　サポートされているアカウントの種類
　　[この組織ディレクトリのみに含まれるアカウント(既定のディレクトリのみ － シングルテナント)]を選択します。
　リダイレクトURI
　　入力不要です。

1．アプリケーションの登録
Microsoft 365のAzure Active Directoryに、本サービスを
アプリケーションとして登録します。

手順２　検知対象となるメールサーバーの参照権限をCWSSに付与します。

1．Azure Portalに，Microsoft 365の管理者権限を持つ組織アカウントでサインインします。
2．[Azure Active Directory] － [アプリの登録]を選択します。
3．手順１で登録したアプリケーションを選択します。
4．[概要] － [APIアクセスの許可の表示]を選択します。
5．[構成されたアクセス許可] － [アクセス許可の追加]を選択します。
6．[APIアクセス許可の要求]で、[Microsoft API]タブの[Microsoft Graph]を選択します。
7．[アプリケーションに必要なアクセス許可の種類]で、[アプリケーションの許可]を選択します。
　以下の３つのアクセス許可を追加します。
　・Directory.Read.All
　・Mail.Read
　・User.Read.All
8．[概要] － [APIアクセスの許可の表示]を選択します。
9．[構成されたアクセス許可]で[サブスクリプション名に管理者の同意を与えます]を選択します。
　サブスクリプション名は、ご使用のサブスクリプションに合わせて読み替えてください。
10．[管理者の同意の確認を与えます。]のメッセージが表示されるので、[はい]を選択します。
11．[概要]を選択し、画面に表示されている**以下の情報を控えてください**。この後の手順で利用します。
　・**アプリケーション（クライアント）ID**
　・**ディレクトリ（テナント）ID**

2．アクセス許可の付与
手順１．で登録したアプリケーションに、電子メールサービスの
参照権限を付与します

※画像内、CWSSはクラウドワークロードセキュリティサービスの略称です

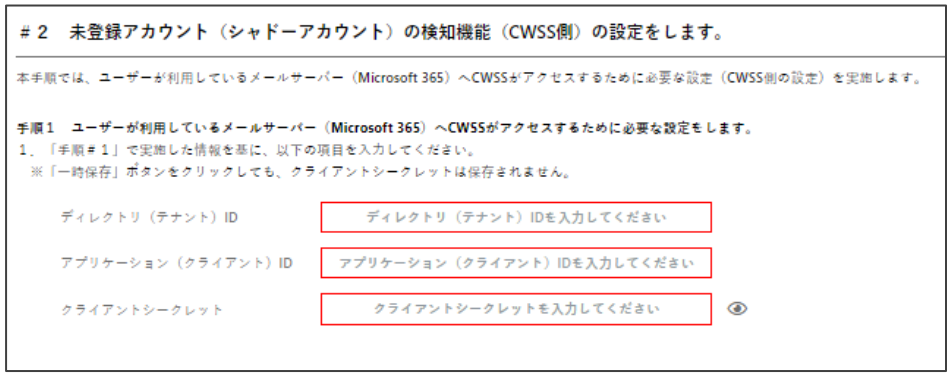
【補足】お客様所有のシステムに追加する設定内容の詳細③～Microsoft 365～

HITACHI
Inspire the Next

手順３　CWSSに登録するクライアントシークレットを作成します。

1．[Azure Active Directory] – [アプリの登録]を選択します。
2．手順１で登録したアプリケーションを選択します。
3．[証明書とシークレット]を選択します。
4．[新しいクライアントシークレット]を選択します。必要な項目を入力し、[追加]を選択します。
　説明
　　クライアントシークレットの説明を入力します。
　有効期限
　　クライアントシークレットが有効な期間を選択します。
5．画面に表示されている、**クライアントシークレットの値を控えてください**。この後の手順で利用します。
　注意
　クライアントシークレットの有効期限が切れると、未登録アカウント（シャドーアカウント）の検知に失敗します。
　その場合は、新しいクライアントシークレットを作成して、再度本サービスに登録する必要があります。

３．クライアントシークレットの作成
本サービスに登録するクライアントシークレットを作成します。
後の手順で、作成したクライアントシークレットを本サービスに登録します。



※画像内、CWSSはクラウドワークロードセキュリティサービスの略称です

HITACHI
Inspire the Next

END

クラウドワークロードセキュリティサービス
トライアル簡単導入ガイド

HITACHI

Inspire the Next