HITACHI
Inspire the Next

クラウドワークロードセキュリティサービス
ご紹介資料

株式会社日立ソリューションズ

CWSS_intro22-11-001

HITACHI
Inspire the Next

Contents

HITACHI
Inspire the Next

Contents

なぜ今、クラウドセキュリティが必要か？

HITACHI
Inspire the Next

事故が多発

近年クラウドに
まつわる事故が多発

・外部公開をしているシステムも多く、
サイバー攻撃に晒されやすい。

・従来のサーバー対策では通用しない
セキュリティリスクがあるため、
セキュリティの専門家でないと
問題点を発見できない。

被害が甚大

情報量やできることも
多いため被害が甚大

・事故発生後の株価は平均6.3%下落※

・年商1,000億円企業における個人情報
漏洩による金銭被害額は12億円
ビジネス停止による機会損失額は
５営業日あたり20億円※

資産の未把握

全社にシステムが
いくつあるか不明

・事業部門が直接調達するため、
情報セキュリティ部門は全社でどのくらい
システムがあるのか把握できない。

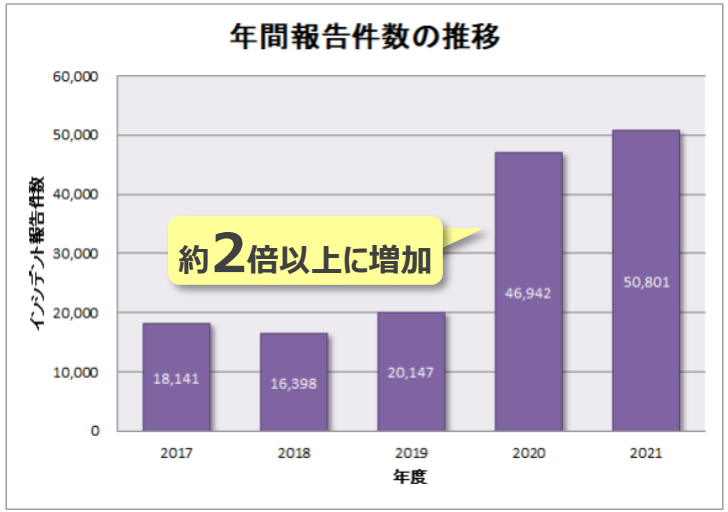
・システム構成は事業部門からの
自己申告が多く、情報セキュリティ部門は
変更点のリアルタイムな把握ができていない。

出典：一般社団法人日本サイバーセキュリティ・イノベーション委員会（JCIC）
(https://www.j-cic.com/pdf/report/Security-Resources-Report.pdf)

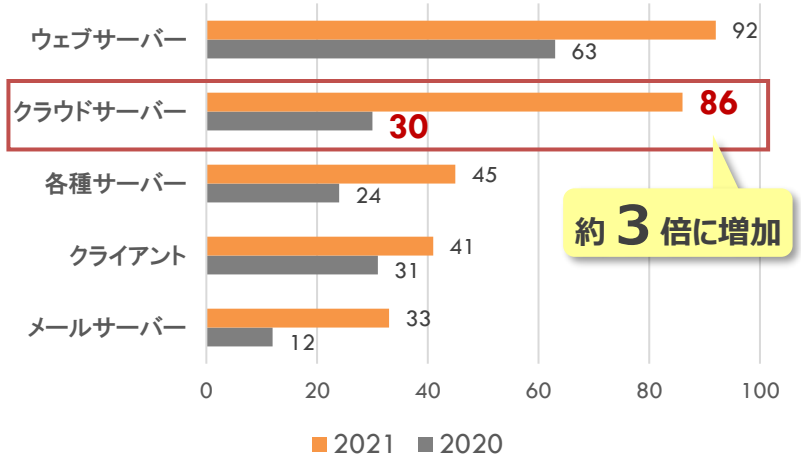
セキュリティインシデントの発生状況

2020年度のセキュリティ事故は前年度の倍以上
クラウドが対象の事故は３倍以上

セキュリティインシデント報告件数



不正アクセス行為の対象となった電算機別件数



（出典）一般社団法人JPCERTコーディネーションセンター
「JPCERT/CC インシデント報告対応レポート 2022年1月1日 ～ 2022年3月31日」
（https://www.jpcert.or.jp/pr/2022/IR_Report2021Q4.pdf）

（出典） 情報処理推進機構（IPA）
「コンピュータウイルス・不正アクセスの届出状況［2021年（1月～12月）］」
P.11 図2-7：不正アクセス電算機別件数の推移（2019～2021）をもとに作成
（https://www.ipa.go.jp/files/000095860.pdf）

補足 情報セキュリティ監査人による警鐘

HITACHI
Inspire the Next

働き方やシステム環境の変化に伴い、リスクそのものが変化
従来のままのセキュリティ対策では十分ではないことを示唆するトピックが多い

順位	情報セキュリティトレンドの内容
1位	緊急コロナ対策からWithコロナへ 業務優先で後回しにしたセキュリティの再点検
2位	多様化するワークスペースに対応するセキュリティ対策
3位	ICTサプライチェーンにおける情報セキュリティリスクの増大
4位	広がるWeb会議利用の盲点 データ漏洩に注意
5位	ISMSからサイバーセキュリティ対策マネジメントへ
6位	個人データ活用におけるビジネスとプライバシーの対立
7位	クラウドの仕様変更への対応不備によるセキュリティ事故
8位	管理機能が攻撃対象に 社外端末によるシステム管理に潜む重大脆弱性
9位	クラウド相互乗り入れ問題 バタフライエフェクトで自社の業務が停止する
10位	気を付けよう外部サービスの穴

出典：「監査人の警鐘 - 2022年 情報セキュリティ十大トレンド」（NPO日本セキュリティ監査協会（JASA））
（https://www.jasa.jp/seminar/sec_trend2022/）

どんなセキュリティ事故が起こっているか？

HITACHI
Inspire the Next

	事例① Amazon Simple Storage Service（Amazon S3）の設定ミスを狙った攻撃	事例② 認証情報の管理不備と過剰権限	事例③ OSSの脆弱性を狙った攻撃
企業	Amazon S3上のシステムファイルが匿名ユーザーから書き込み可	Webサーバーの環境変数にアクセスキーを格納。アクセスキーに過剰な管理者特権が付与	システムで使用していたApache Log4jに任意コード実行の脆弱性が発覚
ハッカー	AmazonS3上のJavaScriptファイルを改ざんし、ファイルを実行すると情報を他サイトへ送信	ミドルウェアの脆弱性を使って環境変数のアクセスキーを不正入手。侵入し仮想通貨のマイニング実行	Javaを使用しているシステムであればApache log4jを使っている可能性が高いため、httpのリクエストを細工し、手あたり次第攻撃を実施
被害	クレジットカード情報が流出	プロバイダーから高額請求され、システムの破棄・作り直し	全世界のサイトが攻撃を受け多くの企業で緊急対策実施

RDP：Remote Desktop Protocol , OSS：Open Source Software
Amazon Simple Storage Serviceの提供元はAmazon.com, Inc.です。

このような課題はありませんか？

HITACHI
Inspire the Next

管理者不在または不明瞭

システム管理者の連絡先などを
正確に把握できていないため
インシデント発生時の迅速な対応が困難

資産情報の散財

システムのセキュリティ点検・監査に
関するさまざまな情報が一元的に
管理されていないため、インシデントの
解決に必要な情報が不十分

同件・類似見直しが困難

リソース（Amazon EC2、AWS Lambdaなど）の
システム単位での管理が不十分なため
インシデント発生時の影響範囲が分かりにくい

このような問題を放置してしまうと

ルート権限奪取

アクセスキーに
ルートレベルの権限が
与えられてしまっている

機密情報漏洩

Amazon S3の
ストレージバケットが外部に
公開されてしまっている

サーバー乗っ取り

Amazon EC2のサーバーへ
誰でもSSH接続が
できる状態になっている

基幹システムへの足がかり

トライアル利用などの
Amazon EC2サーバーが
意図せず放置されている
（シャドーIT）

Amazon EC2 : Amazon Elastic Compute Cloud
Amazon EC2，　AWS Lambdaの提供元はAmazon.com, Inc.です。

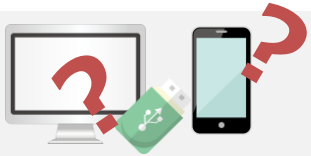
シャドーITとシャドーアカウント

HITACHI
Inspire the Next

クラウド利用の増加に伴い、シャドーITが発生する場面も増えています

管理者が**把握・管理していない**
IT機器やクラウドサービス

→ シャドーIT



クラウド上では…

トライアルアカウントの放置など

→ **シャドーアカウント**

無償トライアルを
会社を通さず契約

- 勝手にサービスを利用される
- 不正ログインされサイバー攻撃の踏み台に
- 脆弱性が放置されマルウェア感染

これらのリスクを発生させないためには
シャドーアカウントを漏れなく把握する必要があります

HITACHI
Inspire the Next

Contents

私たちが着目したコトとは？

HITACHI
Inspire the Next

01

調達資産の
見える化

クラウド上にあるシステムが
どのくらいあるのか
全数が把握できていない

02

セキュアな
環境の維持

クラウド上にあるシステムが
今**正常**な状態なのか
誰が管理しているのか不明

私たちが着目したコトとは？

HITACHI
Inspire the Next

01

調達資産の
見える化

クラウド上にあるシステムが
どのくらいあるのか
全数が把握できていない

シャドーアカウントの警鐘

- ✓ 会社が所有するクラウドアカウントの全数を把握できていない。
- ✓ トライアルなど、会社が利用を把握していない
  アカウント（シャドーアカウント）が放置されている可能性がある。

アカウント乗っ取りの可能性

代替手段にも課題

- ✓ プロキシのログなどから分析するも、
  正常利用のアカウントとの区別もつけにくいうえ、
  利用者を特定できない場合がある。
  （アクセス元のIPアドレス、AWS･Azureなどの
  コンソールURL、アクセス日時しか分からないなど）

AWS：Amazon Web Services，Azure：Microsoft Azure

私たちが着目したコトとは？

HITACHI
Inspire the Next

セキュアな状態の可視化

- ✓ 会社が所有する全システムがセキュアな状態かどうかが一目で分からない。
- ✓ 開発環境など、頻繁に設定を変更するシステムのリスクの変化（新しいリスク）が迅速に把握できない。

システムを安全な状態に保てない

代替手段にも課題

- ✓ 会社が所有するシステムの情報をExcelで管理しているため、得られる情報は基本的に現場からの報告ベースになる。
そのため、リスクの増加や長期間の放置、管理者の変更などを迅速かつ正確に把握することが困難。

02

セキュアな環境の維持

クラウド上にあるシステムが
今正常な状態なのか
誰が管理しているのか不明

プロダクトコンセプト

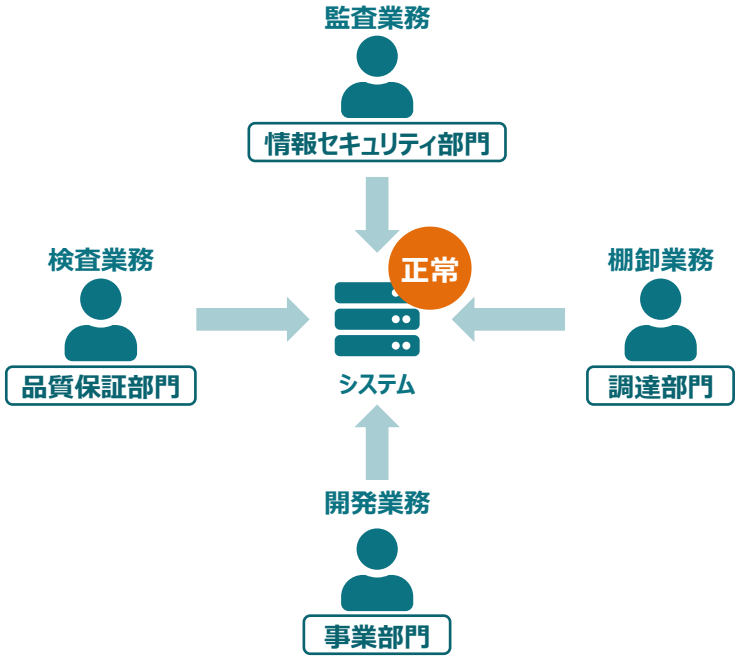
HITACHI
Inspire the Next

「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

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

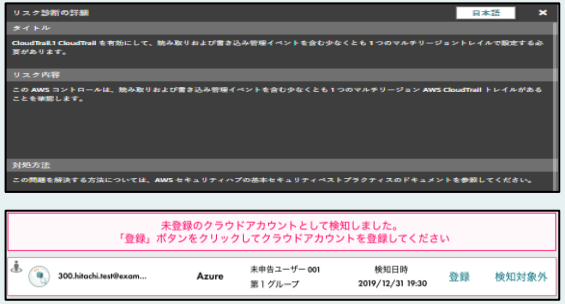
Azure

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

※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とは

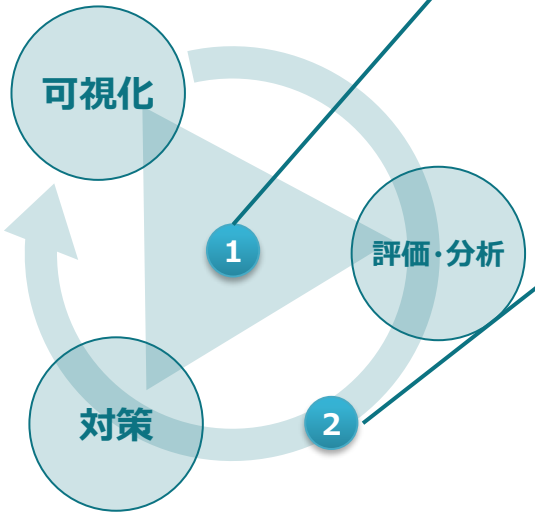
HITACHI
Inspire the Next

事前防衛策となるポスチャマネジメント（CSPM）を支援するツール

事前防衛策

ポスチャマネジメント

セキュリティ侵害を未然に防止
自律的な管理を実現するための仕組み



① CSPM

CSPMをカバーすることで、
クラウド特有のさまざまな攻撃を未然に防ぐ

自社開発アプリ、データ

CWPP　ワークロード保護
（OS、ライブラリ、コンテナ、サーバーレスなど）

CSPM　クラウドインフラ設定
（PaaS、ネットワーク、ストレージ、IAMなど）

② システム統制基盤

全社のシステムの管理情報を一元的に集約し、
ポスチャマネジメントサイクルの好循環を実現

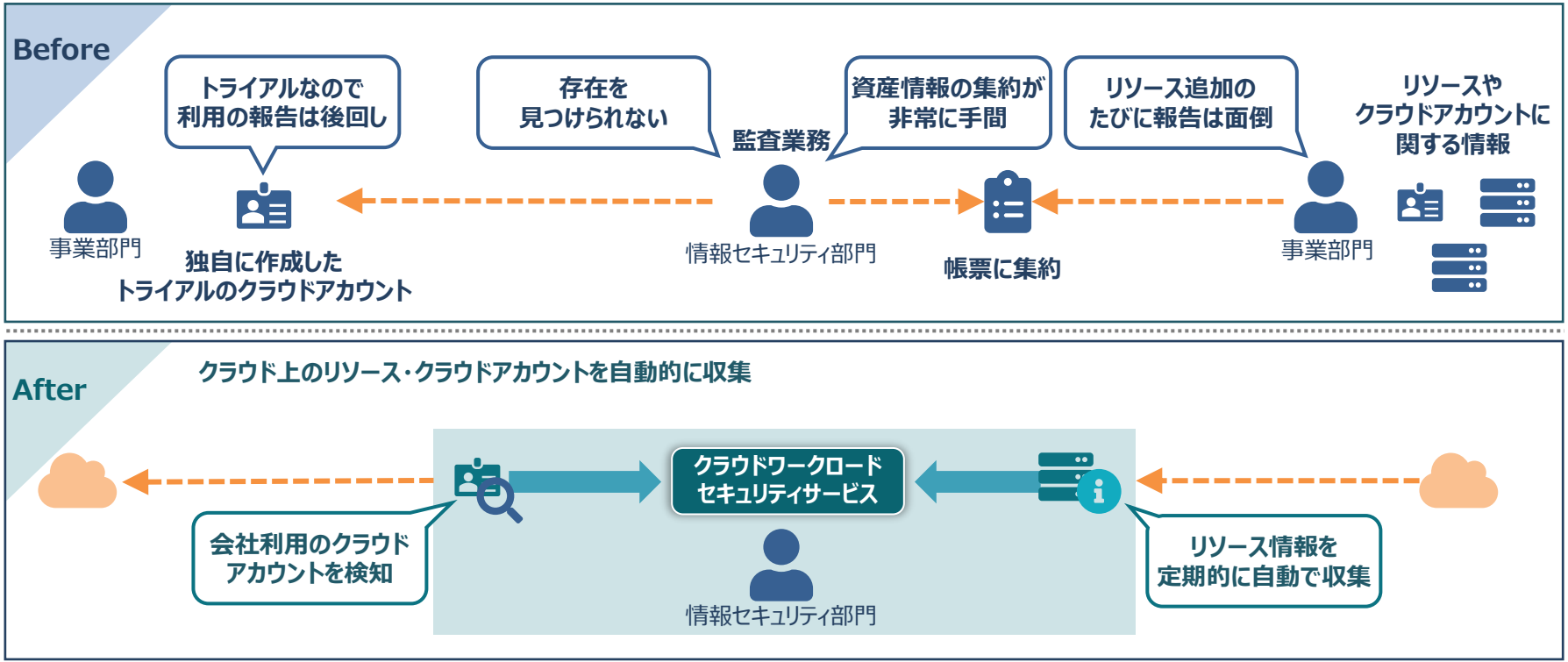
- 点検・監査を迅速化するシステム情報
- システム管理者の連絡先などの担当者情報
- アラートの即時発報や対策のステータス管理

CSPM：Cloud Security Posture Management，CWPP：Cloud Workload Protection Platform
PaaS：Platform as a Service，IAM：Identity and Access Management

クラウドワークロードセキュリティサービスのコアバリュー①

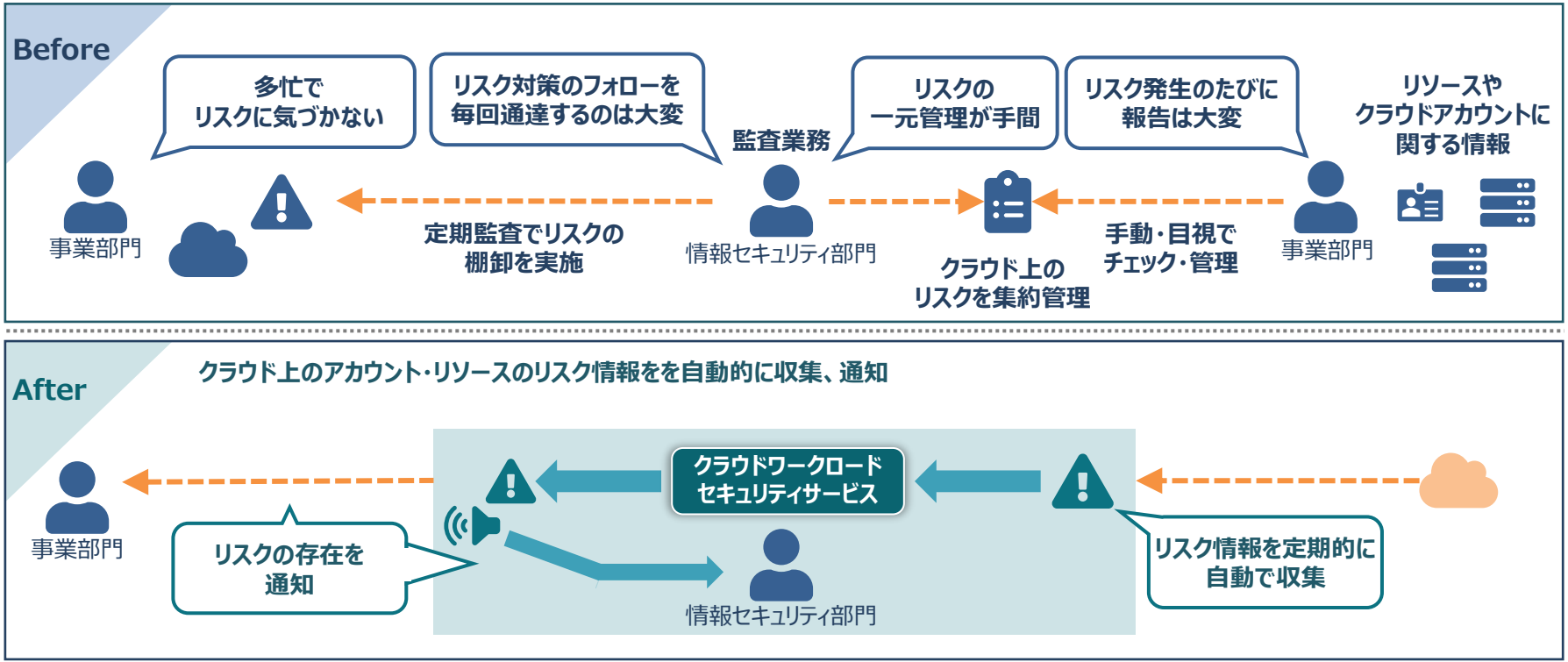
HITACHI
Inspire the Next

全数把握



クラウドワークロードセキュリティサービスのコアバリュー②

常態監視



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

Contents

クラウドワークロードセキュリティサービスによる課題解決

HITACHI
Inspire the Next

管理者不在または不明瞭

システム管理者の連絡先などを
正確に把握できていないため
インシデント発生時の迅速な対応が困難

資産情報の散財

システムのセキュリティ点検・監査に
関するさまざまな情報が一元的に管理
されていないため、インシデントの
解決に必要な情報が不十分

同件・類似見直しが困難

リソース（Amazon EC2、AWS Lambdaなど）の
システム単位での管理が
不十分なためインシデント発生時
の影響範囲が分かりにくい

クラウドワークロードセキュリティサービスがあれば

**仮想リソースの
可視化・一元管理**

仮想リソースを一元管理し
管理対象とリスク状況が
すぐ分かる

セキュリティの自動診断

リスクの内容と対策が
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

シャドーアカウントの検知

会社に申告せずに利用している
クラウドアカウントを検知可能

ユースケース

HITACHI
Inspire the Next

#	想定する企業・部署	BEFORE	AFTER（CWSS導入後）
1	事業部門	利用しているクラウド上のファイルストレージで、**アクセスに必要なID認証を無効（不要）に設定**したことにより、誰でもストレージ上のファイルが閲覧できる状態となり**情報漏洩が発生**。	セキュリティ設定の不備による**脆弱性を自動的に検出・警告**し、**問題点と推奨対策を案内**します。
2		複数システムで脆弱性検知とアラートがあがったが、どのシステムのどこから対処していいか分からない。	リスクの内容だけでなく、**事業の重要度から対策を優先度付け**してご案内。企業にとってクリティカルなシステムから優先的に対策をすることで、事業を止めません。
3	情報システム部門 情報セキュリティ部門	トライアル用に事業部で作成した**アカウントが放置**されており、**不正ログインされサイバー攻撃の踏み台**となってしまった。会社に未申告のアカウントのため、セキュリティ棚卸ではみつからなかった。	会社に**未申告で作成したトライアルアカウント（シャドーアカウント）もCWSSが検知。情報システム部門が知らないIaaS・PaaSの利用を撲滅**し、どの部署の誰が利用しているかを適切に管理が可能です。
4		グループ会社のIaaS・PaaSの利用状況が把握できていない。	グループ会社含め、企業が所有している**システム・仮想リソースを可視化**し、全体像を把握。**インシデント発生時にすばやく対象のシステムを所有している部門に連絡が可能**で、迅速な初動対応を実現します。

IaaS：Infrastructure as a Service
※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

Contents

導入イメージ ～ 全体概要 ～

HITACHI
Inspire the Next

1 本サービスのユーザー情報の設定

Azure ADに登録されている
ユーザー情報（氏名、部署名など）を、
CWSSのユーザー情報と同期します。
※CSVからインポートする方法も
あります。

お客様所有の
Azure AD

接続設定

2 シャドーアカウント検知の設定

お客様所有の
Microsoft 365
のメールボックス

接続設定

アカウント作成時の返信メール、
定期的な請求書メールから特徴を読み取り、
CWSSに未登録のクラウドアカウントと
その作成者を検知します。

クラウドワークロード セキュリティサービス

4 アラート通知の設定

Microsoft Teamsと連携することにより、
リスク検知した際のアラートを
Microsoft Teamsの指定のチャネルに
通知できるようになります。

接続設定

お客様所有の
Microsoft Teams

3 リソース情報収集・リスク検知の設定

接続設定

お客様所有の
AWS, Azure

リスク検知を実施したいAWS, Azureの
クラウドアカウントへの接続情報を設定し、
クラウドアカウントに紐づく
リソース・リスク情報を自動的に収集。

※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

導入イメージ①　～ CWSSのユーザー情報の設定 ～

HITACHI
Inspire the Next

STEP 1

お客様所有のAzure AD

ユーザー情報の同期対象となる
Microsoft 365側の設定をします

Microsoft 365の
Azure ADに
アプリケーション
（CWSS）を登録

検知対象となる
Azure ADの
参照権限を
CWSSに付与

CWSSに登録する
クライアント
シークレットを作成

STEP 2

CWSS　お客様所有の本サービスのテナント

ユーザー情報を収集するための
CWSS側の設定をします

お客様所有のAzure ADへ
CWSSがアクセスするために必要な
クライアントシークレットなどをCWSSに設定

※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

導入イメージ②　～ シャドーアカウント検知の設定 ～

HITACHI
Inspire the Next

STEP 1

お客様所有のMicrosoft 365の
メールボックス

シャドーアカウントの検知対象となる
Microsoft 365側の設定をします

Microsoft 365の
Azure ADに
アプリケーション
（CWSS）を登録

検知対象となる
メールサーバーの
参照権限を
CWSSに付与

CWSSに登録する
クライアント
シークレットを作成

STEP 2

CWSS　お客様所有の本サービスのテナント

シャドーアカウント検知機能に関する
CWSS側の設定をします

お客様所有のメールサーバーへ
CWSSがアクセスするために必要な
クライアントシークレットなどをCWSSに設定

※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

導入イメージ③　～ リソース情報収集・リスク検知の設定 ～

※ 以下の例はAWSの場合の手順を紹介しています。

STEP 1

お客様所有のAWS

本サービスがお客様のAWSにアクセスする
ためのIAMアカウントを作成します

IAMアカウントを
作成するための
設定ファイルを
ダウンロード

設定ファイルを
利用して
IAMアカウントを
作成

STEP 2

お客様所有の
本サービスのテナント

本サービスがAWSに接続するための
接続情報を登録します

お客様所有のAWSへ
CWSSがアクセスするために必要な
Role ARNやExternalIDなどを
CWSSに設定

STEP 3

お客様所有のAWS

リソース情報の収集やリスク検知するために
必要なサービスを有効化します

リソース情報の収集やリスク検知をするために
必要なAWSのサービス（AWS Config /
AWS Security Hub　など）を有効化します

※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

導入イメージ④　～ アラート通知の設定 ～

HITACHI
Inspire the Next

STEP 1

お客様所有のMicrosoft Teams

リスクを検知した際のアラートを受信する
Microsoft Teams側の設定をします

お客様所有のMicrosoft Teamsに
CWSSがアラートを投稿するための
チャネルを作成

STEP 2

CWSS　お客様所有の本サービスのテナント

リスクを検知した際、リスク情報をアラートとして
Microsoft Teamsへ投稿するための設定をします

お客様所有のMicrosoft Teamsへ
CWSSが投稿するために必要な
接続情報の設定（Webhook）をCWSSに設定

※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

価格表

プラン名	想定カバー範囲		各プランの アセットレンジ	最小アセット価格 （年額）	最大アセット価格 （年額）
	部署数	システム数			
12カ月無償トライアルプラン	1部署	5システム	1 ～ 50	¥0	¥0
スタータープランA	1部署	5システム	1 ～ 50	¥960,000	¥960,000
スタータープランB	4部署	20システム	1 ～ 200	¥1,440,000	¥1,440,000
アセット 500	10部署	50システム	201 ～ 500	¥1,454,400	¥5,760,000
アセット 600	12部署	60システム	501 ～ 600	¥5,772,000	¥6,960,000
アセット 700	14部署	70システム	601 ～ 700	¥6,969,600	¥7,920,000
アセット 1000	20部署	100システム	701 ～ 1000	¥7,926,000	¥9,720,000

上記以外のアセット数については下記URLよりご確認ください。

クラウドワークロードセキュリティサービス
価格
https://www.hitachi-solutions.co.jp/cloud_orchestrator/lp/

※アセット数は、VM・コンテナ・サーバーレスの数を表します。

動作環境

HITACHI
Inspire the Next

■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）

RBAC：Role Based Access Control

HITACHI
Inspire the Next

Contents

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

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

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

END

クラウドワークロードセキュリティサービス
ご紹介資料

HITACHI

Inspire the Next