HITACHI
Inspire the Next

IaaS/PaaS向けクラウドセキュリティサービス

Orca Securityのご紹介

株式会社 日立ソリューションズ・クリエイト

Orca_intro23-12-001

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

HITACHI
Inspire the Next

Contents

HITACHI
Inspire the Next

Contents

近年のサイバー攻撃の手口

HITACHI
Inspire the Next

その1 ランサムウェアの悪質化（二重脅迫）

ファイル暗号化に加え、**暗号化前に被害企業のデータを窃取**
一部を公開し、身代金を払わないとデータを暴露すると二重に脅迫
業務停滞だけでなく、**顧客からの信用も失墜**

その2 VPN製品の脆弱性を狙った攻撃

VPN製品の脆弱性や**ファームウェア更新不備**を突き、社内ネットワークに侵入
テレワークの普及で**VPN利用が増えた**ことにも起因

その3 クラウドサービスを狙った攻撃

クラウドの設定不備や**脆弱性対策不備**を突き、クラウドに侵入

VPN：Virtual Private Network

IaaS/PaaSで起こるセキュリティインシデント

HITACHI
Inspire the Next

事例 1　Amazon S3の設定ミスを狙った攻撃

企業側

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

ミス

ハッカー

Amazon S3上のJavaScriptファイルを改ざん
ファイルを実行すると情報を他サイトへ送信

クレジットカード情報が流出

Amazon S3：Amazon Simple Storage Service [スケーラビリティ、データ可用性、セキュリティ、およびパフォーマンスを提供するオブジェクトストレージサービス]（提供元：Amazon.com, Inc）

IaaS/PaaSで起こるセキュリティインシデント

HITACHI
Inspire the Next

事例 2　通信制御の設定ミスを狙った攻撃

企業側

急ぎだし
今日だけなら･･･

クラウドは変更が容易なことが多い

メンテナンスのため一時的にRDPポートの通信を許可

ミス

ハッカー

ツールで発見！
(数時間でハッキング)

ポートスキャンツールで即発見！攻撃対象に！

顧客情報漏えい

RDP：Remote Desktop Protocol

IaaS/PaaSで起こるセキュリティインシデント

HITACHI
Inspire the Next

事例 3　認証情報の管理不備と過剰権限

企業側

環境変数は
便利

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を付与

ミス

ミス

ハッカー

環境変数なら
覗きやすいぞ

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

プロバイダーから高額請求
システムの破棄・作り直し

環境変数：Webサーバー上のプログラムが参照することのできる変数のこと。
サーバーの設定に関する情報や、プログラミング環境の情報、アクセスユーザに関する情報などが含まれます。

IaaS/PaaSで起こるセキュリティインシデント

HITACHI
Inspire the Next

事例 4　OSS(オープンソース)の脆弱性を狙った攻撃

企業側

リリース時に診断を実施しているので安心

Apache Log4jをシステムで使用
しかし、**Log4jに任意コード実行の脆弱性が発覚**
(2021年12月)

CVSSスコア10.0

ハッカー

この脆弱性は簡単に利用できる！

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

**全世界のサイトが攻撃を受けており
多くの企業で緊急対策実施中**

OSS：Open Source Software , CVSS：Common Vulnerability Scoring System

HITACHI
Inspire the Next

事例5 クラウド設定ミスによる顧客情報漏えいの可能性

インシデント発生組織

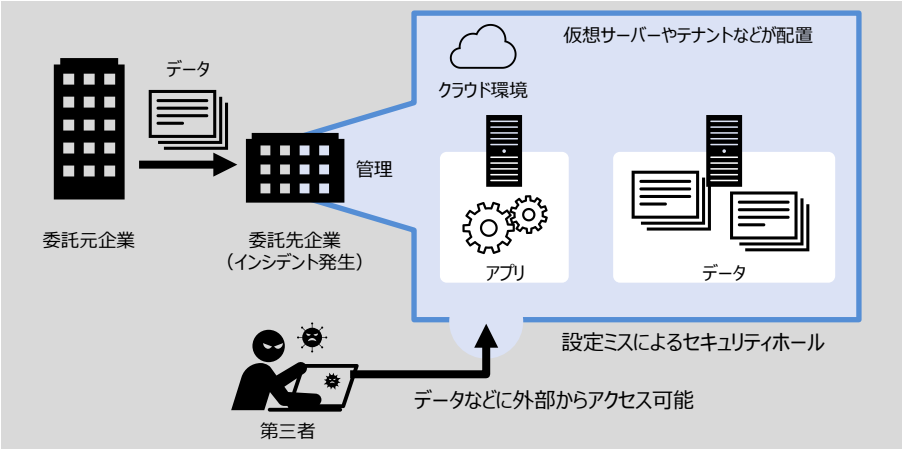
- 製造業関連でデータ管理の委託を受けていたIT企業

被害

- およそ215万人のユーザーに関する以下の情報
  車載端末、車台番号、車両位置情報、時刻

インシデントの概要

2015年2月～2023年5月の間、クラウド環境の設定ミスにより、お客さま情報を含むデータの一部が、外部からアクセス可能な状態にあった。
一部海外向け環境では、個人情報もアクセス可能であった。



結果

- 顧客情報漏えいの可能性のある顧客へ個別に連絡
- 専用コールセンター設置
- 再発防止の検討およびクラウド監査システムの導入
- 対策・対応のためのコストは非公開
- **政府の個人情報保護委員会が行政指導**

HITACHI
Inspire the Next

Contents

クラウドでセキュリティ事故が起こる原因

HITACHI
Inspire the Next

3つの原因

原因1 開発環境や検証環境で油断

原因2 初回は入念に対策するが、メンテナンスで緩む

原因3 クラウドサービスの進化に知見が追い付かない

最近よく聞く事故の傾向①

HITACHI
Inspire the Next

開発環境や検証環境で油断
～開発環境や検証環境が原因で事故が起こりがち～

インターネットに公開していないし・・・

顧客情報は置いていないし・・・

実は・・・

- 設定ミスで外部公開
- OS・ミドルウェアの脆弱性を放置
- 利便性優先で簡易なパスワードを設定

ハッカーにとっては・・・

侵入が容易

本番環境の設定が推測できる

仮想通貨のマイニングに悪用

最近よく聞く事故の傾向②

HITACHI
Inspire the Next

初回は入念に対策するが、メンテナンスで緩む
～システムの改修やメンテナンス時の設定変更でミス～

メンテナンスのため
通信ポートを一時的に開放

プログラムの認証キーに
過剰な権限を付与

システムの改修・メンテナンスサイクル(CI/CD)

OS、ミドルウェアの
セキュリティパッチ適用が遅れる

新たなOSSライブラリーを使い
脆弱性が混入

CI/CD : Continuous Integration/Continuous Delivery(Continuous Deployment), OSS : Open Source Software

最近よく聞く事故の傾向③

HITACHI
Inspire the Next

クラウドサービスの進化に知見が追い付かない

便利なサービスを手探りで活用


Amazon S3


AWS Lambda
(ラムダ)

- 匿名ユーザーからのアクセスを許可
- 意図せずインターネット公開

自社プログラム用に認証キーを作成

- 認証キーが外部に露出
- 管理者特権が付与されていて何でもできてしまう

AWSでは1年に1,000件以上のサービス提供や機能アップデートあり

AWSのセキュリティ設定例

Amazon S3	AWS Lambda	コンテナ
● 公開範囲 ● 読み書き権限 etc.	● 実行権限を極小化 ● アクセスキーを秘匿化 etc.	● コンテナ作成権限の制限 ● コンテナエスケープ対策　etc.

AWS Lambdaの提供元はAmazon.com, Incです。サーバーをプロビジョニングまたは管理せずにコードを実行できるようにするコンピューティングサービスです。

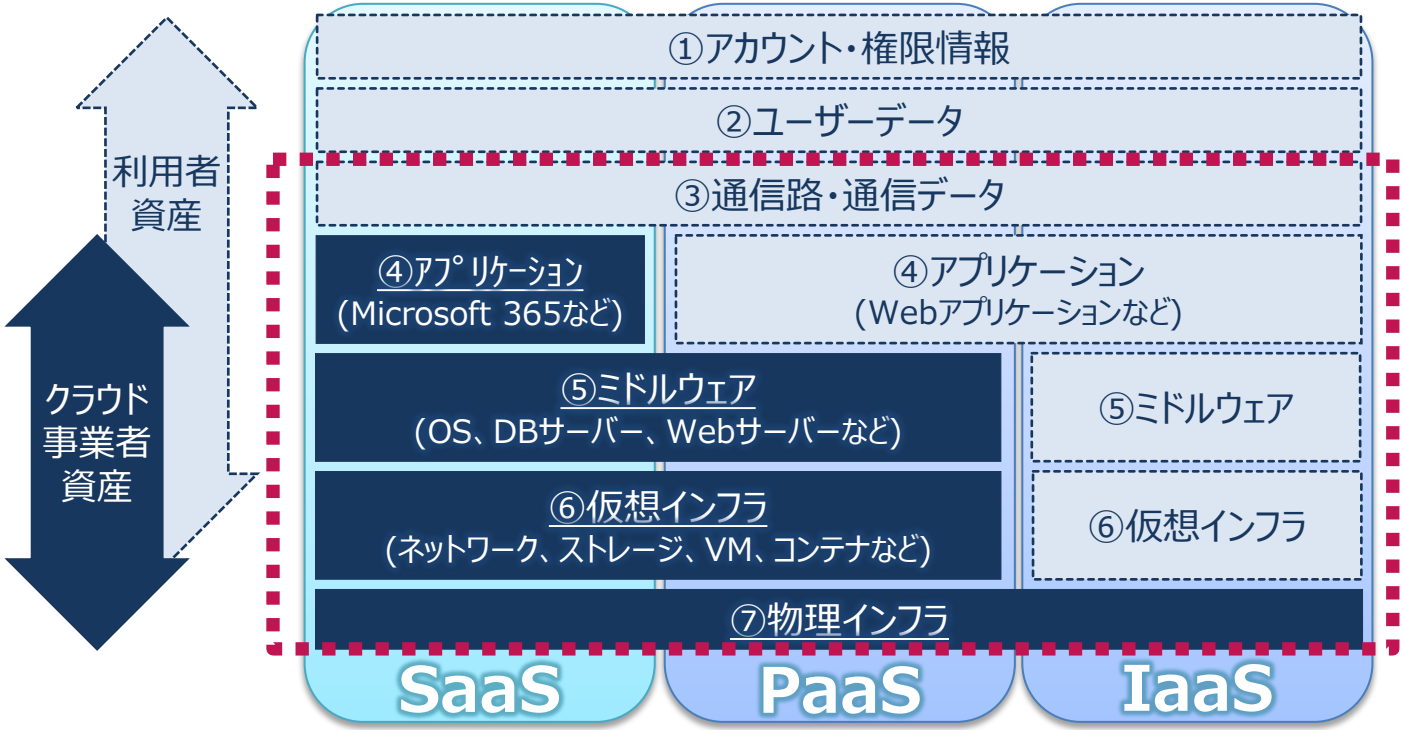
HITACHI
Inspire the Next

Contents

クラウドの責任共有モデル

HITACHI
Inspire the Next

アカウント情報やデータなどは利用者責任のため セキュリティ対策の検討が必要



凡例：

- 事業者が提供・運用する範囲
- 利用者が導入・運用する範囲

責任共有モデルとは、サービスにおける責任をクラウド事業者と利用者との間で共有する考え方で、IaaS、PaaS、SaaSの責任分界点によって異なる。

参考：CSA(Cloud Security Alliance)によるクラウドサービスのシステム階層

IaaS/PaaSで必要なセキュリティ対策

HITACHI
Inspire the Next

：攻撃を受けないためにやること
：攻撃を受けた時のためにやること

レイヤー	対策すべき項目			
データ	機密データ管理・暗号化	ラテラルムーブメント対策		
アプリケーション	ライブラリー脆弱性	アプリケーション認証	Webアプリケーション脆弱性	
OS, ミドルウェア	脆弱性 (CVE)	OS・ミドルウェア 認証	パッチ適用	期限切れ
	マルウェア	サーバーレス 設定	コンテナ設定	
インフラ （基盤）	認証 (IAM)	ネットワーク 設定	暗号化設定	ログ取得 設定
	ストレージ アクセス設定	キーコンテナ アクセス設定	ベンダー固有 サービス設定	アラート 設定

CVE:Common Vulnerabilities and Exposures, IAM: Identity and Access Management

対策のポイント

HITACHI
Inspire the Next

3 つのポイント

ポイント 1 仮想リソースを全て可視化

- IaaS/PaaS上の全仮想リソースの可視化がスタートライン

ポイント 2 脆弱性・設定ミスの点検を自動化

- 人手での点検は形骸化する
- クラウドの機能アップデートに技術者の知見が追い付かない

ポイント 3 運用の負担が少ない方を選ぶ

- 診断ツールの設定・導入が簡単でないと徹底できない
- アラートがトリアージされない診断ツールは運用がまわらない

HITACHI
Inspire the Next

Contents

Orca Security　４つの特長

HITACHI
Inspire the Next

CSPM･CWPP･CIEMの機能を網羅し、パブリッククラウドのセキュリティリスクを継続的に自動検出

広範囲のリスクを診断

エージェントレスで
本番環境への影響なし

数分で簡単導入

ノイズが少なく
運用がラク

対象はAWS, Azure, Google Cloud Platform（以降、GCP）

CSPM:Cloud Security Posture Management, CWPP:Cloud Workload Protection Platform, CIEM:Cloud Infrastructure and Entitlements Management

Google Cloud Platformの提供元はGoogle LLCです。

特長①広範囲のリスクを診断

HITACHI
Inspire the Next

：Orca Securityのチェック範囲

：チェック範囲外

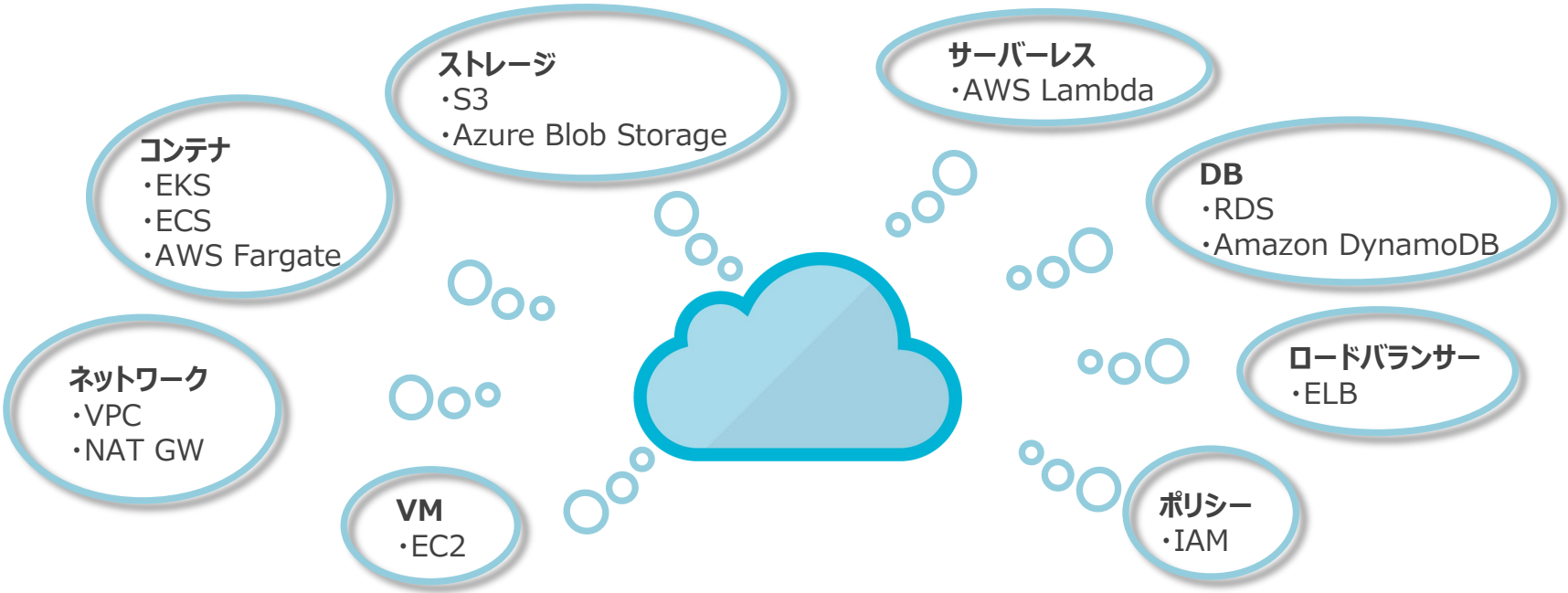
レイヤー	対策すべき項目			
データ	機密データ管理・暗号化	ラテラルムーブメント対策		
アプリケーション	ライブラリー脆弱性	アプリケーション認証	Webアプリケーション脆弱性	
OS, ミドルウェア	脆弱性 (CVE)	OS・ミドルウェア 認証	パッチ適用	期限切れ
	マルウェア	サーバーレス 設定	コンテナ設定	
インフラ （基盤）	認証 (IAM)	ネットワーク 設定	暗号化設定	ログ取得 設定
	ストレージ アクセス設定	キーコンテナ アクセス設定	ベンダー固有 サービス設定	アラート 設定

CVE:Common Vulnerabilities and Exposures, IAM: Identity and Access Management

特長①広範囲のリスクを診断

HITACHI
Inspire the Next

クラウドネイティブな資産も可視化が可能



EKS：Amazon Elastic Kubernetes Service, ECS：Amazon Elastic Container Service
S3：Amazon Simple Storage Service, RDS：Amazon Relational Database Service, IAM：Identity and Access Management
VPC：Amazon Virtual Private Cloud, NAT GW：Network Address Translator gateway
EC2：Amazon Elastic Compute Cloud, ELB：Elastic Load Balancing

特長①広範囲のリスクを診断

HITACHI
Inspire the Next

クラウドのセキュリティをさらに広範囲にカバー

その1 CIEM (Cloud Infrastructure Entitlement Management)

不要なアカウントが放置されていたり、権限がきちんと管理されていないことをチェックし、
クラウド環境への不正侵入のリスクの低減を実現できます。

その2 DevSecOps (Shift left)

IaCツールやCI/CDツールと連携し、本番適用前に設定コードのセキュリティを
自動チェックできるため、安全な環境構築や運用コストの低減を実現できます。

その3 APIセキュリティ

APIの構成ミスとセキュリティリスクを特定することで、クラウドのAPIを介して
セキュリティ侵害を受けるリスクの低減を実現できます。

特長②エージェントレスで本番環境への影響なし

HITACHI
Inspire the Next

：攻撃を受けないためにやること
：攻撃を受けた時のためにやること

レイヤー	対策すべき項目			
データ	機密データ管理・暗号化		ラテラルムーブメント対策	
アプリケーション				ﾟリケーション脆弱性
OS, ミドルウェア				期限切れ
	マルウェア	サーバーレス 設定	コンテナ設定	
インフラ （基盤）	認証 （IAM）	ネットワーク 設定	暗号化設定	ログ取得 設定
	ストレージ アクセス設定	キーコンテナ アクセス設定	ベンダー固有 サービス設定	アラート 設定

エージェント導入が必要な場合が多い

特長②エージェントレスで本番環境への影響なし

HITACHI
Inspire the Next

性能に影響なく、本番環境を止めずに導入・検査が可能

お客さま環境

Orca Security社 スキャナー

Orca Security社 環境

①スナップショットを作成

②スキャン実行

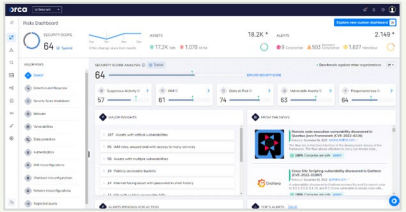
③リスクや仮想リソース情報を送信

仮想環境

仮想環境

一時領域

Orca Security スキャナー

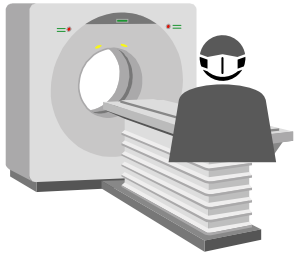


④ダッシュボードに表示

同一のリージョン内で実施

HITACHI
Inspire the Next

Orca SecurityはクラウドのMRI検査



身体にメスをいれることなくMRI装置でスキャン

腫瘍などのリスクを可視化。
投薬・手術などの対応については医師と相談のうえ、決定

Orca Security

お客さま環境はエージェントレスで
複製した環境に対して外部からスキャン

アセットとリスクを可視化。
診断結果から対策内容までダッシュボード上で確認可能

MRI:Magnetic Resonance Imaging

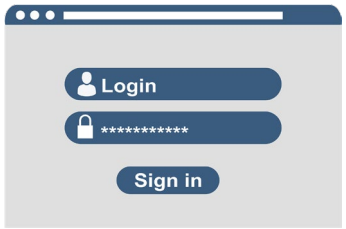
特長③数分で簡単導入

HITACHI
Inspire the Next

わずか 3 ステップ
クラウドアカウントに最初に１度設定するだけ

■AWSの例

STEP 1



AWSにログイン

STEP 2

テンプレート実行

STEP 3

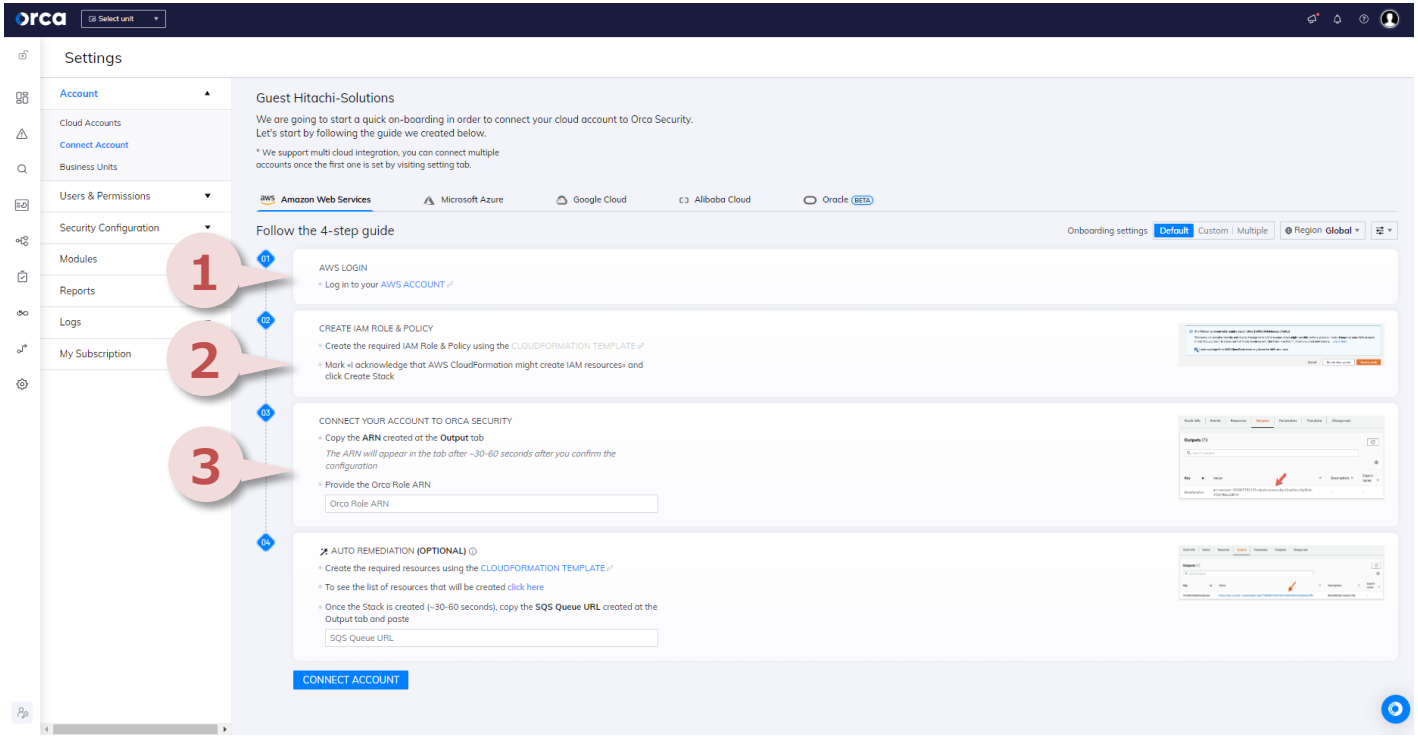
本サービスと連携

設定完了後、約１日後にはチェックが完了します。
また、継続して、日々自動的にチェックを実施します。

特長③数分で簡単導入

HITACHI
Inspire the Next

わずか 3 ステップ
クラウドアカウントに最初に１度設定するだけ

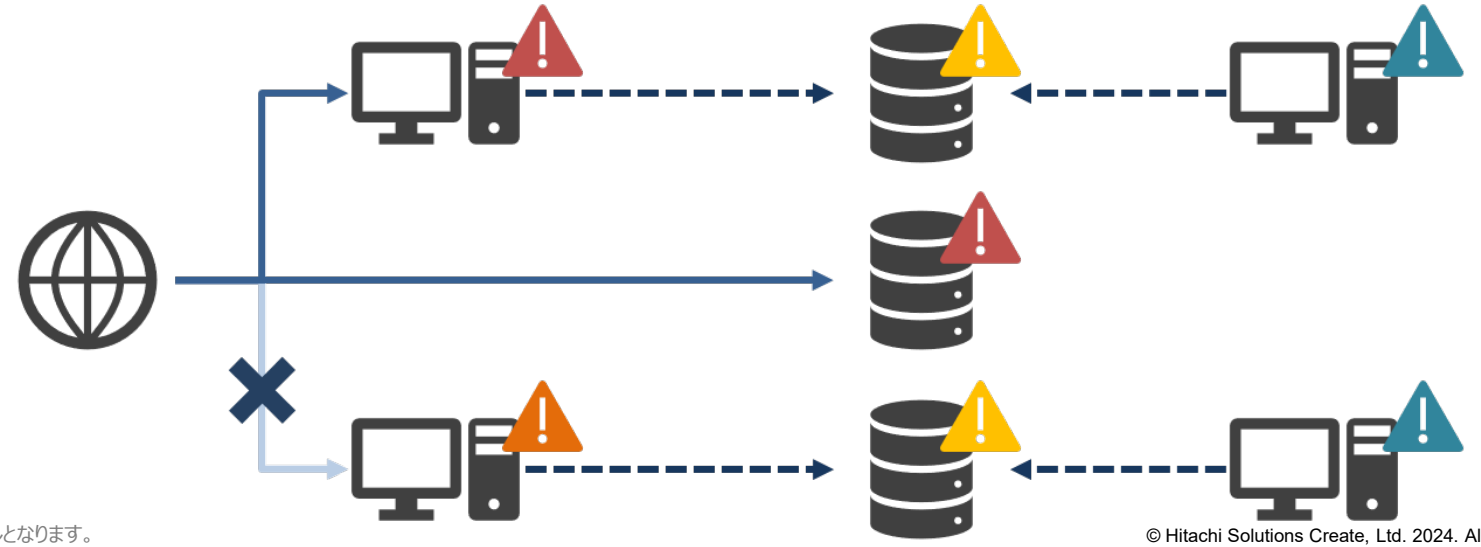


特長④ノイズが少なく運用がラク

HITACHI
Inspire the Next

インターネットからの到達可能性も加味し、自動で優先度付け
優先度に従って対応することで、負荷なく効率的に運用できる

リスク高	リスク中	リスク低	Information
2件	5件	20件	3,000件



※記載の数値はサンプルとなります。

HITACHI
Inspire the Next

Orca Securityならではのスマートな分析結果

脆弱性やリスクそれぞれの一般的な緊急度合いだけで曖昧な点数を出すのではなく、
関連する全てのクラウドアセットの性質やつながりを分析した上で優先度を付けます

- リスク本来の一般的な緊急度
- 外部ネットワークの到達性
- ラテラルムーブメントリスク
- リソースに対するアクセスの範囲と権限
- 攻撃対象のビジネスインパクト　など

緊急度の低いリスクを後にし、真に致命的なものから効率よく対策できる！
対象環境の特性上、致命的なリスクを見逃さない！

HITACHI
Inspire the Next

Contents

Q.収集した情報は安全に守られていますか？

HITACHI
Inspire the Next

ご安心ください
高レベルのセキュリティシステムで安全を確保しています

各種セキュリティ認証を取得

ISO 27017
クラウドサービスセキュリティ
国際規格

ISO 27018
クラウドサービス
個人情報保護国際規格

ISO 27001
情報セキュリティ
マネジメントシステム国際規格

Orca Security

SOC2-TYPE2
クラウドサービス内部統制
国際規格

AWS
US-Verginiaリージョン

OR

AWS
EU-ドイツリージョン

Q.継続的なチェックはなぜ必要ですか？

HITACHI
Inspire the Next

システムの運用・エンハンス・メンテナンスで生じるさまざまなセキュリティ対策不備を迅速に検知し、セキュリティ事故を予防することが重要

システムの改修・メンテナンスサイクル(CI/CD)

運用開始後も、例えば以下のような問題が発生します

- OSSライブラリーやコンテナイメージに脆弱性が混入
- 不要に高い権限をもつユーザーを追加
- ハッカーに狙われやすい環境変数にシークレット情報を保管
- メンテナンスのためにポート開放し、放置
- 退職者のアカウントを放置
- OSSライブラリーの新たな脆弱性が公開

HITACHI
Inspire the Next

Contents

Orca Security社とは

HITACHI
Inspire the Next

Orca Security,Inc

設立	：2018年
本社	：イスラエル
代表者	：CEO…Gil Geron
従業員数	：約500名
資金調達	：総計5億5,000万ドル 投資ラウンド…シリーズC（2021/10時点） Googleの親会社Alphabetの独立系ファンドなどから資金調達
事業内容	：クラウド上のセキュリティサービスを提供
評価額	：18億ドルユニコーン企業（2021/10時点）
導入実績	：金融、IT、エンタープライズ、中規模まで、幅広い業種・規模のお客さまで実績あり

ダッシュボード

HITACHI
Inspire the Next

マルチクラウド環境でもお客さまの資産とリスクを一元管理

主要リスクごとにリスクを一覧

HITACHI
Inspire the Next

リスクをリスクレベルで色分けして一覧表示

アラートの詳細

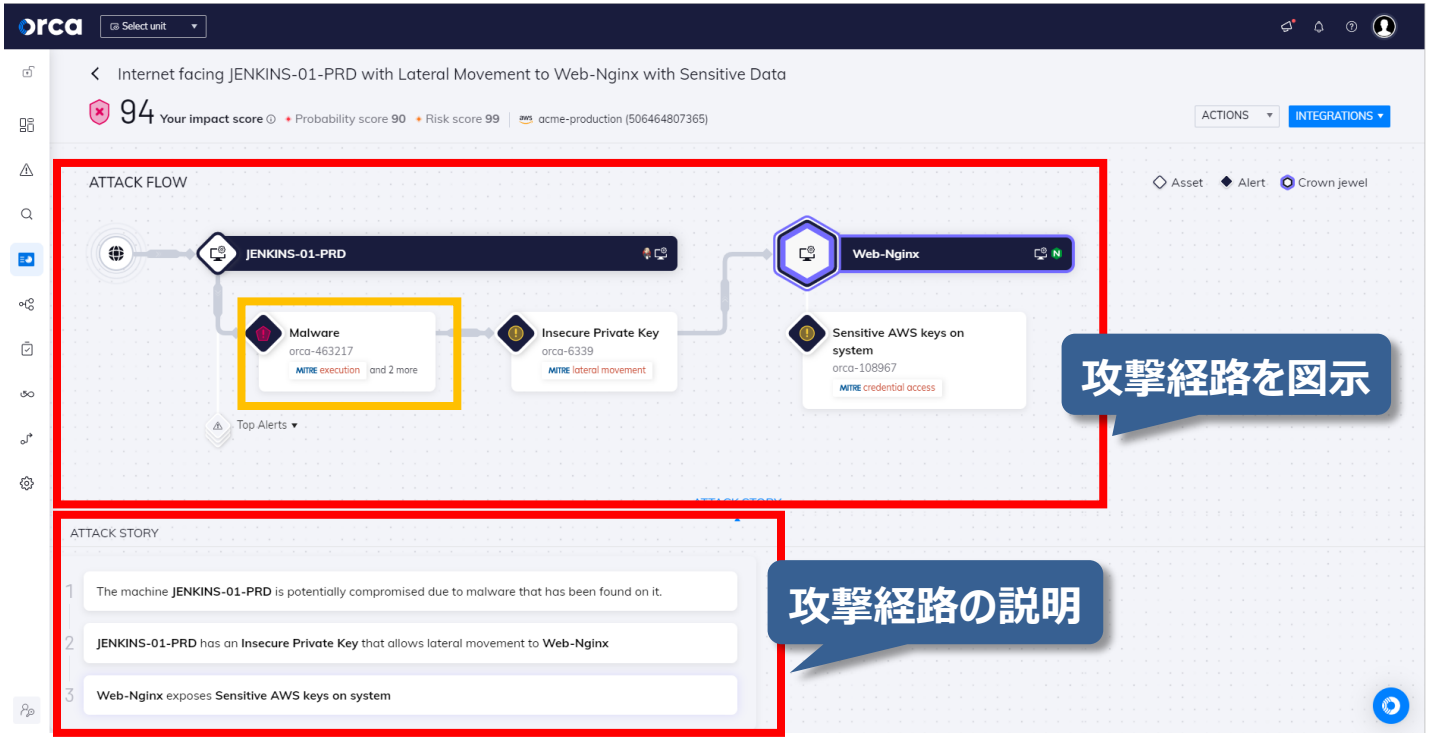
HITACHI
Inspire the Next

診断結果と対処策を提示
資産の攻撃経路や資産の詳細情報も併せて表示

攻撃経路の表示

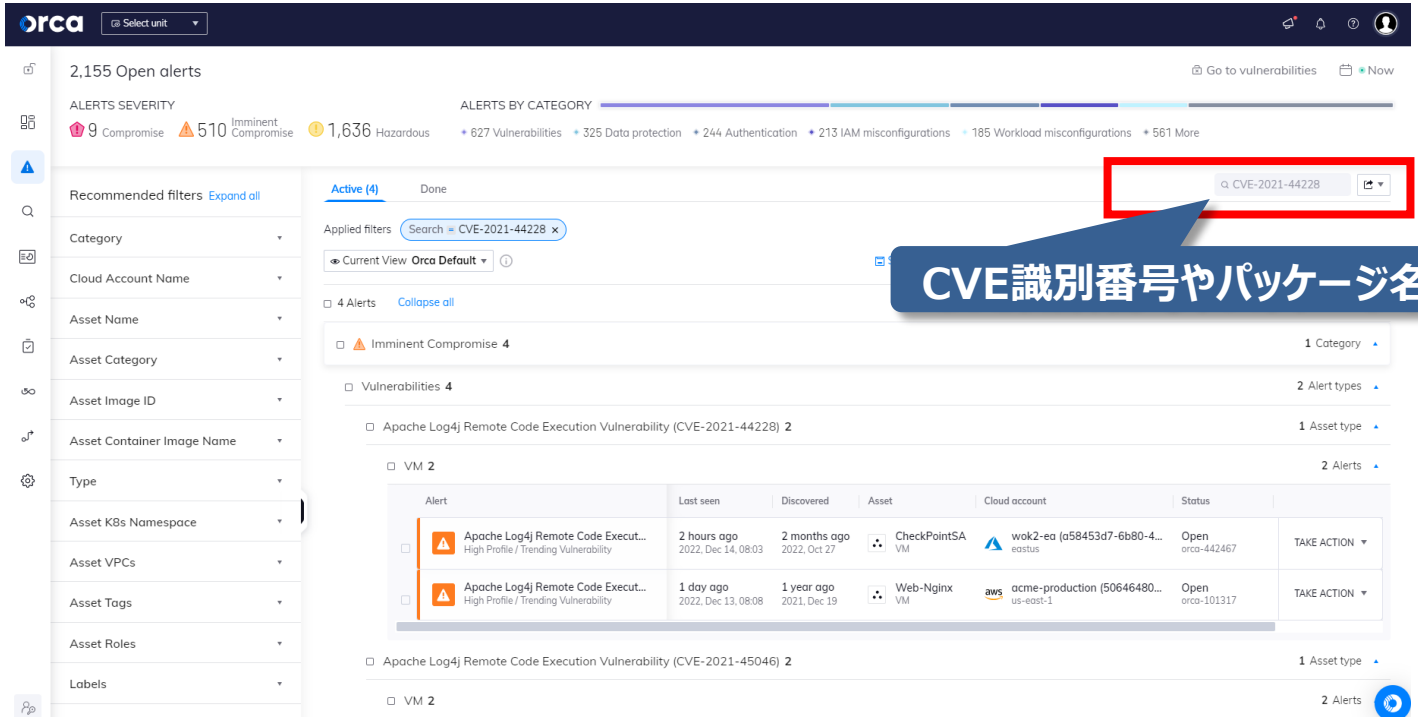
HITACHI
Inspire the Next

脆弱性を組み合わせることによる攻撃リスクを分析可能



HITACHI
Inspire the Next

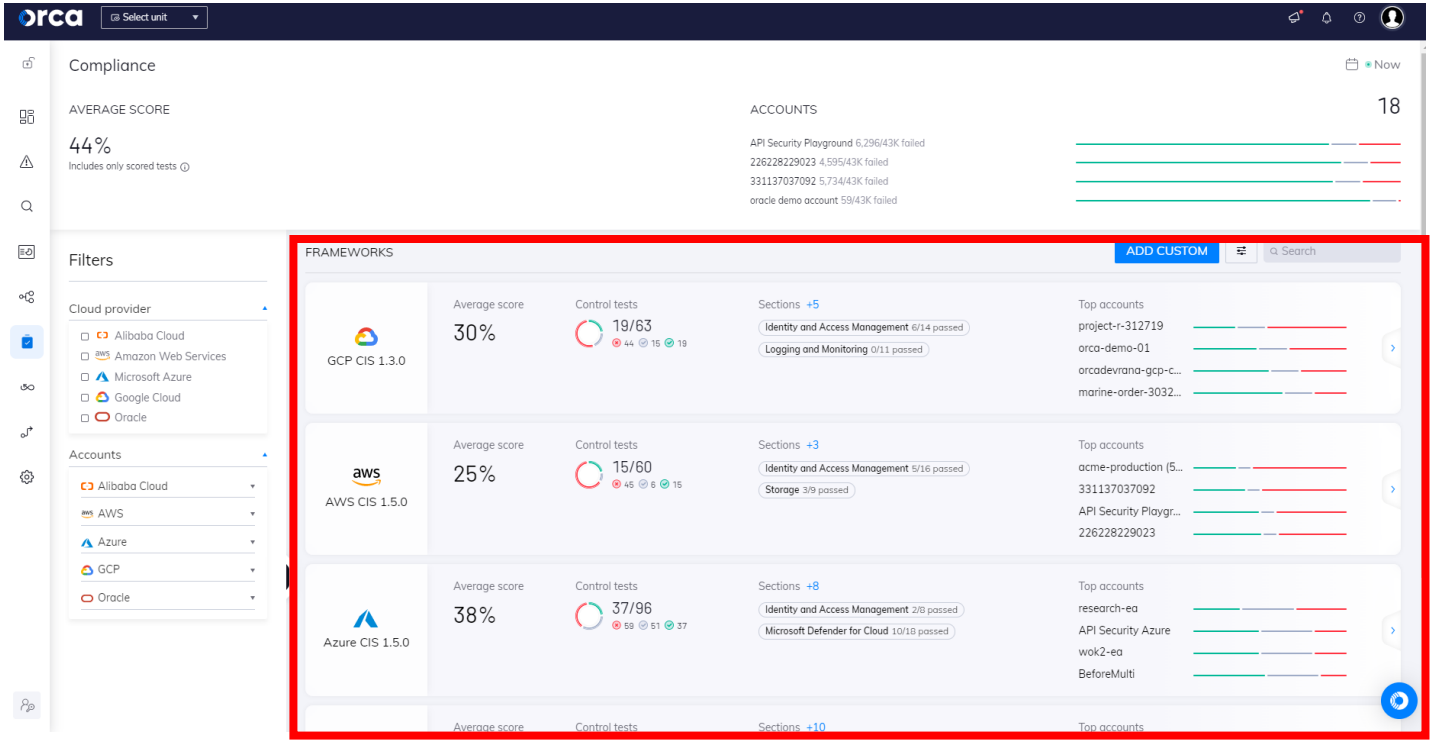
脆弱性を持つシステムを特定可能



コンプライアンス対応

HITACHI
Inspire the Next

各クラウドプロバイダーのCIS、PCI DSSなど、さまざまなコンプライアンス基準を監査可能



CIS:Center of Internet Security，PCI DSS:Payment Card Industry Data Security Standard

お問い合わせ

HITACHI
Inspire the Next

株式会社 日立ソリューションズ・クリエイト

Webでのお問い合わせ

www.hitachi-solutions-create.co.jp/inq.html

お問い合わせページより、商品・サービスをお選びください。

メールでのお問い合わせ

hsc-contact@mlc.hitachi-solutions.com

表示に関する注意事項

HITACHI
Inspire the Next

■他社商品名、商標などの引用に関する表示

- Orca Securityは、Orca Security Ltd.の登録商標です。
- Microsoft Azureは、米国、その他の国における米国Microsoft Corp.の登録商標です。
- Amazon Web Services、Amazon S3 、AWS LambdaはAmazon.com Inc.の登録商標です。
- Google Cloud Platformは、Google LLCの登録商標です。
- その他記載の会社名、製品名は、それぞれの会社の商標もしくは登録商標です。

■サービス・製品の仕様に対する表示

本資料に記載しているサービス・製品の仕様は、2024年7月現在のものです。

サービス・製品の改良などにより予告なく記載されている仕様が変更になることがあります。

■お問い合わせ情報について

お問い合わせ情報についてご相談・ご依頼いただいた内容は回答などのため、
当社の関連会社（日立ソリューションズグループ会社）および
株式会社日立製作所に提供（共同利用も含む）することがあります。
取り扱いには十分注意し、お客さまの許可なく他の目的に使用することはありません。