
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

Contents

1. クラウドサービスを狙うサイバー攻撃
2. セキュリティ事故の傾向
3. 対策のポイント
4. サービスの特長
5. よくあるご質問

付録（Orca Security社のご紹介、画面イメージ）

Contents

1. クラウドサービスを狙うサイバー攻撃
2. セキュリティ事故の傾向
3. 対策のポイント
4. サービスの特長
5. よくあるご質問

付録（Orca Security社のご紹介、画面イメージ）

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

事例 1

Amazon S3の設定ミスを狙った攻撃



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



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

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



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

事例 3

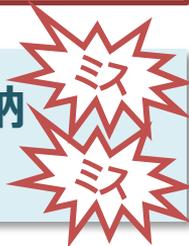
認証情報の管理不備と過剰権限



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



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

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

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

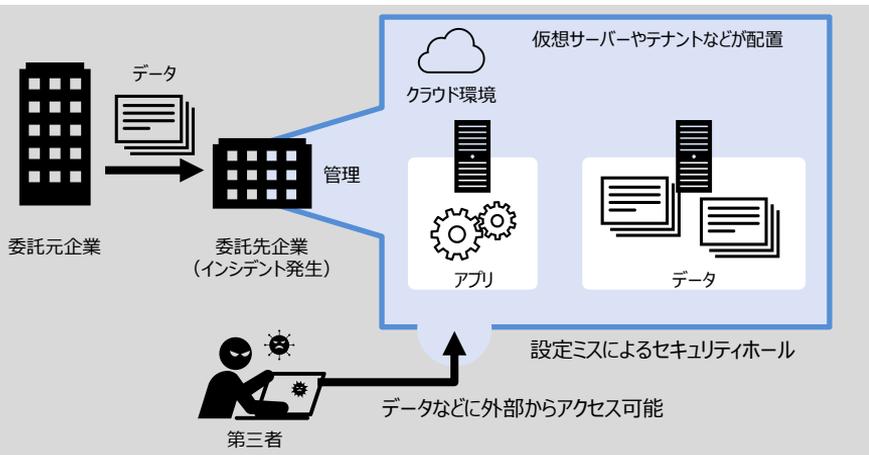
- ☑ 製造業関連でデータ管理の委託を受けていたIT企業

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**

Contents

1. クラウドサービスを狙うサイバー攻撃
2. セキュリティ事故の傾向
3. 対策のポイント
4. サービスの特長
5. よくあるご質問

付録（Orca Security社のご紹介、画面イメージ）

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

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



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

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

- 公開範囲
- 読み書き権限 etc.

AWS Lambda

- 実行権限を極小化
- アクセスキーを秘匿化 etc.

コンテナ

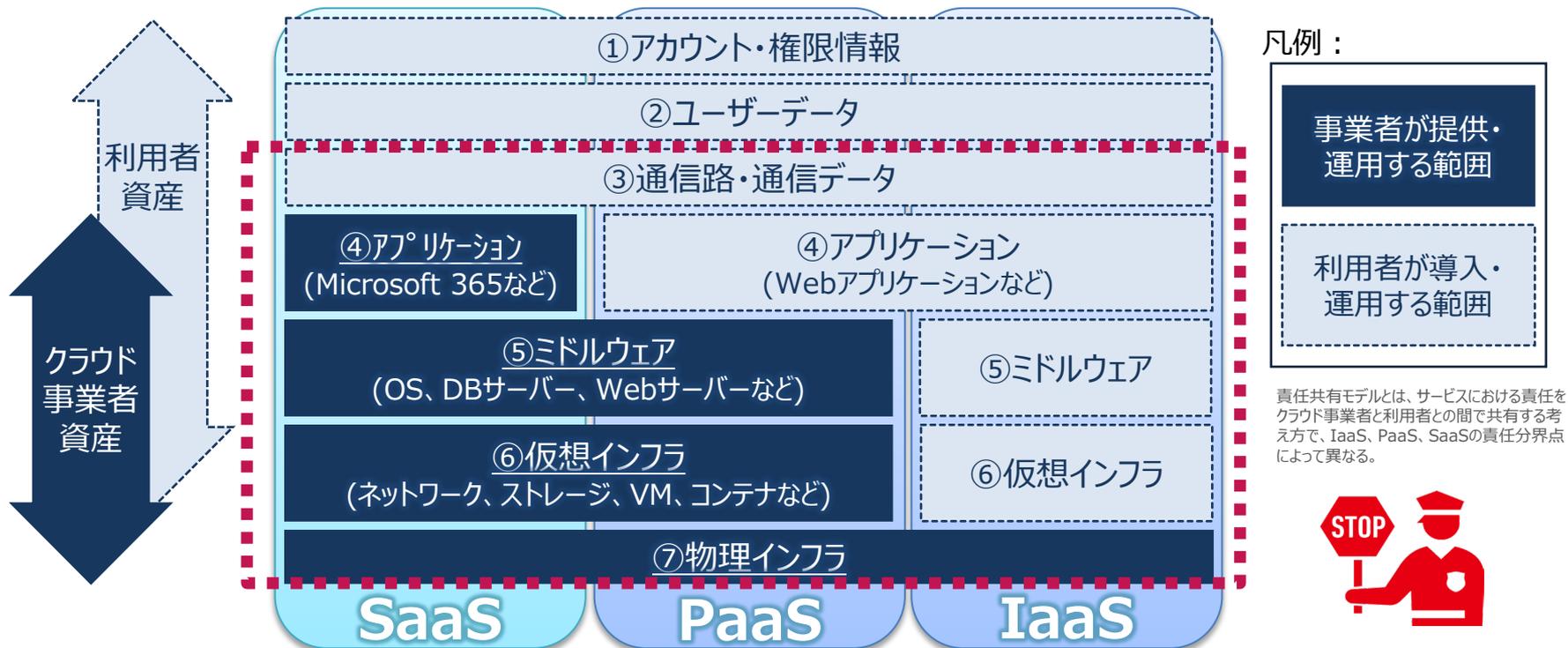
- コンテナ作成権限の制限
- コンテナエスケープ対策 etc.

Contents

1. クラウドサービスを狙うサイバー攻撃
2. セキュリティ事故の傾向
3. 対策のポイント
4. サービスの特長
5. よくあるご質問

付録（Orca Security社のご紹介、画面イメージ）

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



- : 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	<div style="display: flex; justify-content: space-around;"> <div style="border: 1px solid #ccc; border-radius: 10px; padding: 5px; background-color: #c0504d; color: white; text-align: center;">機密データ管理・暗号化</div> <div style="border: 1px solid #ccc; border-radius: 10px; padding: 5px; background-color: #c0504d; color: white; text-align: center;">ラテラルムーブメント対策</div> </div>
アプリケーション	<div style="display: flex; justify-content: space-around;"> <div style="border: 1px solid #ccc; border-radius: 10px; padding: 5px; background-color: #c0504d; color: white; text-align: center;">ライブラリー脆弱性</div> <div style="border: 1px solid #ccc; border-radius: 10px; padding: 5px; background-color: #c0504d; color: white; text-align: center;">アプリケーション認証</div> <div style="border: 1px solid #ccc; border-radius: 10px; padding: 5px; background-color: #c0504d; color: white; text-align: center;">Webアプリケーション脆弱性</div> </div>
OS, ミドルウェア	<div style="display: grid; grid-template-columns: repeat(4, 1fr); gap: 5px;"> <div style="border: 1px solid #ccc; border-radius: 10px; padding: 5px; background-color: #c0504d; color: white; text-align: center;">脆弱性 (CVE)</div> <div style="border: 1px solid #ccc; border-radius: 10px; padding: 5px; background-color: #c0504d; color: white; text-align: center;">OS・ミドルウェア 認証</div> <div style="border: 1px solid #ccc; border-radius: 10px; padding: 5px; background-color: #c0504d; color: white; text-align: center;">パッチ適用</div> <div style="border: 1px solid #ccc; border-radius: 10px; padding: 5px; background-color: #c0504d; color: white; text-align: center;">期限切れ</div> <div style="border: 1px solid #ccc; border-radius: 10px; padding: 5px; background-color: #c0504d; color: white; text-align: center;">マルウェア</div> <div style="border: 1px solid #ccc; border-radius: 10px; padding: 5px; background-color: #c0504d; color: white; text-align: center;">サーバーレス 設定</div> <div style="border: 1px solid #ccc; border-radius: 10px; padding: 5px; background-color: #c0504d; color: white; text-align: center;">コンテナ設定</div> </div>
インフラ (基盤)	<div style="display: grid; grid-template-columns: repeat(4, 1fr); gap: 5px;"> <div style="border: 1px solid #ccc; border-radius: 10px; padding: 5px; background-color: #c0504d; color: white; text-align: center;">認証 (IAM)</div> <div style="border: 1px solid #ccc; border-radius: 10px; padding: 5px; background-color: #c0504d; color: white; text-align: center;">ネットワーク 設定</div> <div style="border: 1px solid #ccc; border-radius: 10px; padding: 5px; background-color: #c0504d; color: white; text-align: center;">暗号化設定</div> <div style="border: 1px solid #ccc; border-radius: 10px; padding: 5px; background-color: #4a7ebb; color: white; text-align: center;">ログ取得 設定</div> <div style="border: 1px solid #ccc; border-radius: 10px; padding: 5px; background-color: #c0504d; color: white; text-align: center;">ストレージ アクセス設定</div> <div style="border: 1px solid #ccc; border-radius: 10px; padding: 5px; background-color: #c0504d; color: white; text-align: center;">キーコンテナ アクセス設定</div> <div style="border: 1px solid #ccc; border-radius: 10px; padding: 5px; background-color: #c0504d; color: white; text-align: center;">ベンダー固有 サービス設定</div> <div style="border: 1px solid #ccc; border-radius: 10px; padding: 5px; background-color: #4a7ebb; color: white; text-align: center;">アラート 設定</div> </div>

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जされない診断ツールは運用がまわらない

Contents

1. クラウドサービスを狙うサイバー攻撃
2. セキュリティ事故の傾向
3. 対策のポイント
4. サービスの特長
5. よくあるご質問

付録（Orca Security社のご紹介、画面イメージ）

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



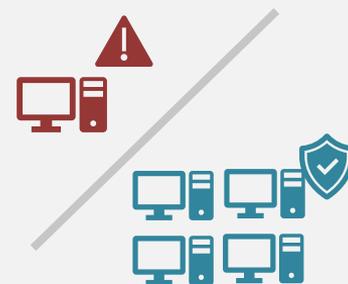
広範囲のリスクを診断



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)

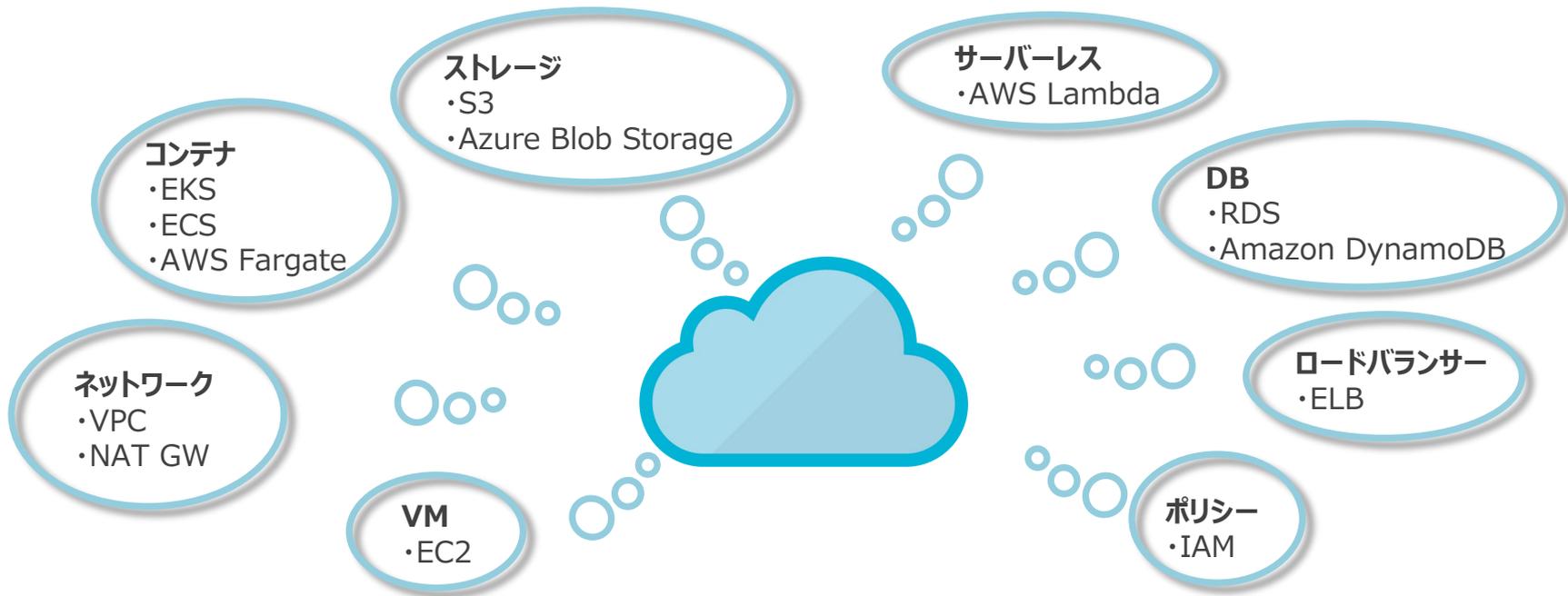
特長① 広範囲のリスクを診断

: 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

クラウドネイティブな資産も可視化が可能



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

- : 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				アプ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**

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

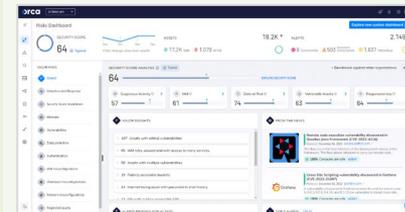


仮想環境

一時領域



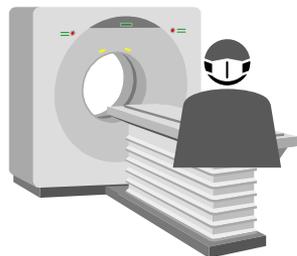
Orca Security
スキャナー



④ダッシュボードに表示

同一のリージョン内で実施

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

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

Orca
Security

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。

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

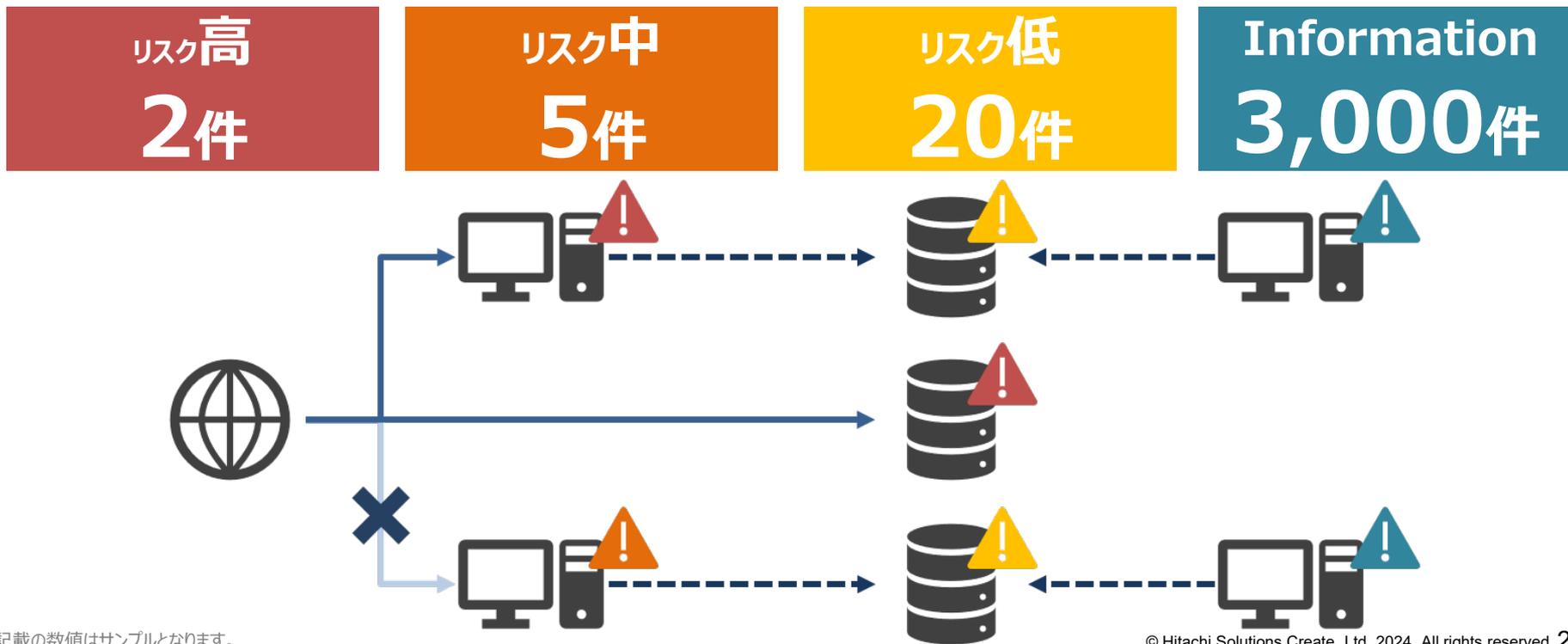
The screenshot shows the Orca Security 'Settings' page. The left sidebar contains navigation options: Account, Cloud Accounts, Business Units, Users & Permissions, Security Configuration, Modules, Reports, Logs, and My Subscription. The main content area is titled 'Guest Hitachi-Solutions' and provides instructions for connecting a cloud account. A 'Follow the 4-step guide' section is visible, with three steps highlighted by red callout bubbles:

- 1** **AWS LOGIN**
Log in to your [AWS ACCOUNT](#).
- 2** **CREATE IAM ROLE & POLICY**
Create the required IAM Role & Policy using the [CLOUDFORMATION TEMPLATE](#).
Mark acknowledge that AWS CloudFormation might create IAM resources and click Create Stack.
- 3** **CONNECT YOUR ACCOUNT TO ORCA SECURITY**
Copy the **ARN** created at the **Output** tab.
The ARN will appear in the tab after ~30-60 seconds after you confirm the configuration.
Provide the Orca Role ARN.

Below the third step, there is an optional section for 'AUTO REMEDIATION (OPTIONAL)'. A 'CONNECT ACCOUNT' button is located at the bottom of the guide.

特長④ ノイズが少なく運用がラク

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



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！

Contents

1. クラウドサービスを狙うサイバー攻撃
2. セキュリティ事故の傾向
3. 対策のポイント
4. サービスの特長
5. よくあるご質問

付録（Orca Security社のご紹介、画面イメージ）

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？

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



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

Contents

1. クラウドサービスを狙うサイバー攻撃
2. セキュリティ事故の傾向
3. 対策のポイント
4. サービスの特長
5. よくあるご質問

付録（Orca Security社のご紹介、画面イメージ）

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

マルチクラウド環境でもお客様の資産とリスクを一元管理



リスクをリスクレベルで色分けして一覧表示

The screenshot displays the Orca security dashboard interface. On the left, a sidebar contains a list of filters such as 'Category', 'Cloud Account Name', 'Asset Name', and 'Type'. A blue callout box labeled '各種条件(VM、AWSなどでフィルタ)' points to this sidebar. The main content area shows a summary of risk levels: 'Active (2,149)', 'Compromise 9', 'Imminent Compromise 503', and 'Hazardous 1,637'. A blue callout box labeled 'リスクレベルで色分け' points to these risk level indicators. A yellow callout box labeled 'リスクレベルごとのアラート一覧' points to a detailed view of 'Malware 9' alerts, which includes a table with columns for 'Alert', 'Last seen', 'Discovered', and 'Asset'. The table lists two malware alerts on a VM asset.

Alert	Last seen	Discovered	Asset
Malware /C:/Users/Administrator/Downloads/mimik...	7 hours ago 2022, Dec 13, 08:08	3 years ago 2020, May 12	Window VM
Malware /var/lib/jenkins/plugins/mailer/mailer.js@mail...	7 hours ago 2022, Dec 13, 08:08	1 month ago 2022, Nov 8	JENKINS- VM

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

診断結果

対処策

対処策やエビデンス、詳細などを表示可能

資産詳細情報

Orca Select unit

Malware (Compromise) Change

Overview Details Evidence Remediations Status & Comments Forensics (BETA)

SUMMARY

We have detected a file infected with Trojan:BitCoinMiner.SX on the asset. The file was detected by the anti-virus engine with high confidence. Additionally, the file was found to be malicious by our intelligence feed with high confidence.

More information regarding malware alert

Name Malware
Category Malware
First seen 11-08-2022 08:00
Last seen 12-13-2022 08:00
Orca ID orca-463217
Ticket # JIRDEMO-330

TAGS malware_found confidence: high

ASSET JENKINS-01-PRD

Overview Details Evidence Remediations Status & Comments Forensics (BETA)

Remove the infected file immediately, and audit your asset and network for any anomalies or other infected files.

Remediation

Remediation console:

1. Remove the infected file immediately.
2. Audit your asset and network for any anomalies or other infected files.
3. In case you are not familiar with the file and further security information is needed, you may search the file hash in [VirusTotal](#).
4. In case the file is not known to the website, you may upload it via [VirusTotal files upload](#), and the file will get scanned by various security vendors. **Important:** Files that are uploaded to VirusTotal must not include proprietary information as these are publicly shared by the website.

17 Similar alerts [View in alerts](#)

JENKINS-01-PRD
AWS EC2 Instance

Last scan Today [Open in AWS](#) [Scan now](#)

Crown Jewel Mark as crown jewel

Tags Name|JENKINS-01-PRD

Observations public_facing brute-force_attempts

Identity

Alerts on asset 2 3 9 250
Internet facing Yes
Attack paths 18 High Impact

Asset ID i-01a93cof3b9bc
Asset type AwsEc2Instance
Cloud account acme-productio...

Asset roles Distro Ubuntu 16.04
Cloud account ID 506464807365

Status Running

[GO TO ASSET](#)

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

The screenshot displays the ORCA security dashboard for the unit 'Internet facing JENKINS-01-PRD with Lateral Movement to Web-Nginx with Sensitive Data'. The dashboard shows a 'Your impact score' of 94, with a probability score of 90 and a risk score of 99. The main section is titled 'ATTACK FLOW' and illustrates a sequence of events: 1. Malware (orca-463217) is found on the JENKINS-01-PRD machine. 2. An Insecure Private Key (orca-6339) is identified on the same machine, which allows for lateral movement to the Web-Nginx service. 3. Sensitive AWS keys are exposed on the Web-Nginx system. A yellow box highlights the Malware node, and a red box encompasses the entire attack flow diagram and the 'ATTACK STORY' section below it. The 'ATTACK STORY' section provides a narrative of the attack path in three steps.

攻撃経路を图示

攻撃経路の説明

1 The machine JENKINS-01-PRD is potentially compromised due to malware that has been found on it.

2 JENKINS-01-PRD has an Insecure Private Key that allows lateral movement to Web-Nginx

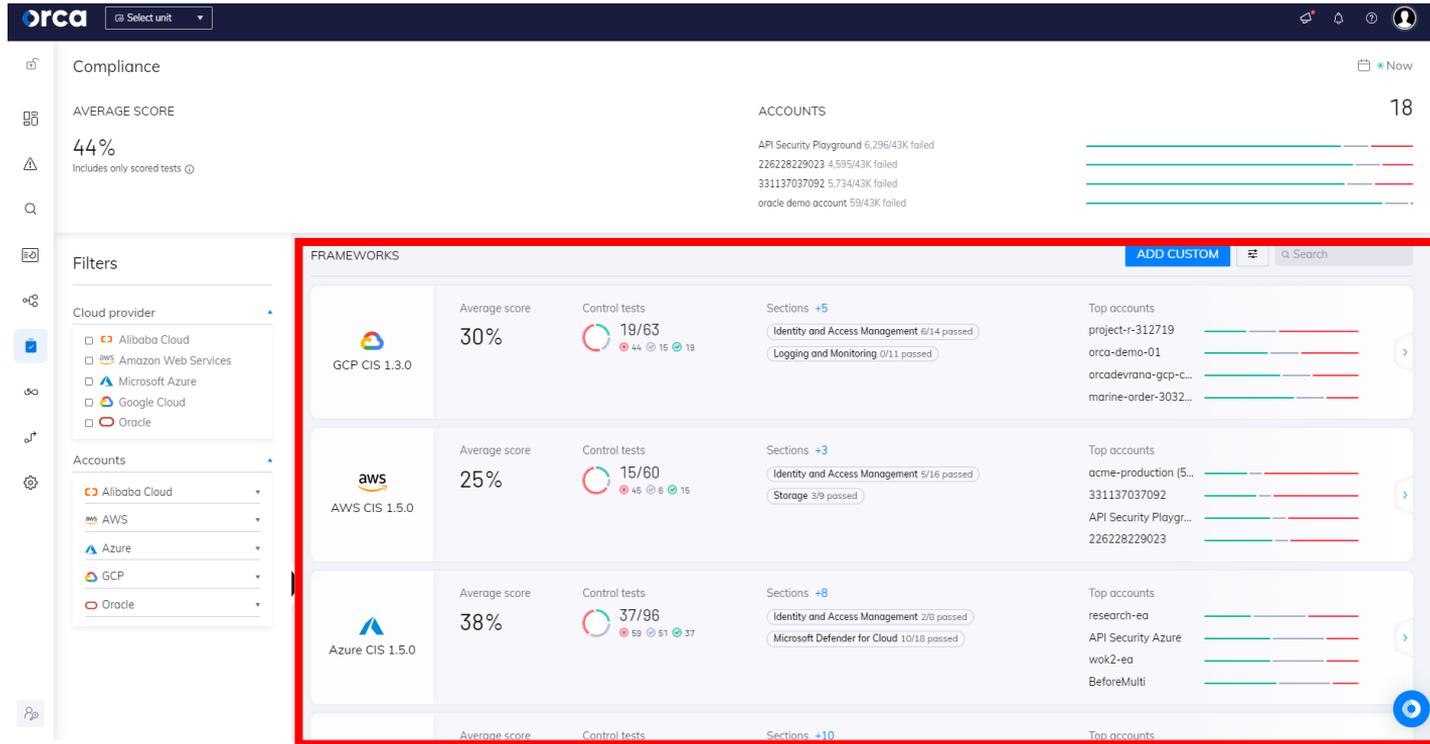
3 Web-Nginx exposes Sensitive AWS keys on system

脆弱性を持つシステムを特定可能

The screenshot shows the Orca vulnerability management dashboard. At the top, it displays '2,155 Open alerts' and 'ALERTS SEVERITY' with counts for Compromise (9), Imminent Compromise (510), and Hazardous (1,636). Below this, there are 'ALERTS BY CATEGORY' and a search bar containing 'CVE-2021-44228'. A blue callout box with white text points to the search bar, stating 'CVE識別番号やパッケージ名で検索' (Search by CVE ID or package name). The main content area shows a list of alerts, including 'Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228) 2' and 'Apache Log4j Remote Code Execution Vulnerability (CVE-2021-45046) 2'. A table of alerts is visible, with columns for Alert, Last seen, Discovered, Asset, Cloud account, and Status.

Alert	Last seen	Discovered	Asset	Cloud account	Status
Apache Log4j Remote Code Execut... High Profile / Trending Vulnerability	2 hours ago 2022, Dec 14, 08:03	2 months ago 2022, Oct 27	CheckPointSA VM	wok2-ea (a58453d7-6b80-4-... eastus	Open orca-442467
Apache Log4j Remote Code Execut... High Profile / Trending Vulnerability	1 day ago 2022, Dec 13, 08:08	1 year ago 2021, Dec 19	Web-Nginx VM	aws acme-production (50646480-... us-east-1	Open orca-101317

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



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

■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。