Cloud Security

BeeX

パブリッククラウドで社内システムを構築されているお客さま！

セキュリティ対策は万全ですか？

クラウド上の何気ない設定や管理の不備が脆弱性に…

クラウドの設定や管理のミスを狙った

サイバー攻撃増加中

- 外部への公開設定
- アカウントの管理
- 通信の許可設定
- アクセスキーの管理

BeeX Propolis

BeeX Propolisとは、クラウドの設定や管理のミスによる脆弱性がないかを診断し診断結果を分析・レポートするサービスです。

各セキュリティテンプレートに基づいた診断

AWS、Microsoft Azue、Google Cloudに対応した様々なセキュリティフレームワークのテンプレートをご用意しております。各テンプレートに基づき診断を実施します。

お客様環境要件を考慮して見解を提示

非準拠項目の対応方針について、記者環境要件を考慮した上で、BeeXの見解をもとに、対処方法をご提示します。

スポット診断及び定期診断をご選択いただけます

スポット診断の場合は、お客様の必要なタイミングで診断分析レポートを提供します。定期診断は、半年ごとに診断を行い、改善策を伴走支援いたします。

BeeX Propolis

複雑化するクラウド環境における設定や管理のミスに対応した診断・改善サービス

Failed Tests Summary

Rule Name	Severity	Tested	Relevant	Non Compliant
Ensure the default security group of every VPC restricts all traffic	High	35	21	21
Ensure MFA Delete is enable on S3 buckets				
Ensure AWS Config is enabled in all regions				
Ensure rotation for customer created CMKs is enabled				
Ensure CloudTrail logs are encrypted at rest using KMS CMKs				
Ensure credentials (with first activated acccessKey) unused for 90 days or greater are disabled				
Ensure VPC flow logging is enabled in all VPCs				
Ensure IAM instance roles are used for AWS resource access from instances				
Ensure first access key is rotated every 90 days or less				

ルール名	Failed有無	重大度	対応	要否理由	対象リソース	備考
S3バケットがHTTPアクセスを明示的に拒否するバケットポリシーがあることを確認する	有	High	要確認	S3バケットにHTTPアクセスを拒否した際の影響を考慮して判断が必要。 また、Failedに該当したS3バケットについては、バケットポリシーでIPアドレス制限を付けている。また、IAMユーザーが各バケットごとに紐づくかたちでアクセスが制限されている。	299のS3バケット	
NACLにおいて、0.0.0.0/0 からサーバ管理用ポートへのインバウンドアクセスを許可しないこと	有	High	否	すでにサーバ単位でアクセス制御を行っている。（サブネットの分割やセキュリティグループでのきめ細やかな設定を行っている。） NACLではサブネット全体に影響があり、かつインバウンドとアウトバウンド双方でそれぞれ設定が必要となり設計も複雑になる。特にインバウンドでエフェメラルポートを利用している場合に通信できなくなる可能性もあるため慎重に判断する必要がある。	すべてのNACL(25)	
EBSが暗号化されていることを確認する	有	High	要	移行環境で利用している既存のEC2にアタッチされているEBSボリュームの暗号化が無効になっている。	すべてのEBSボリューム(24)	
RDSインスタンスの暗号化設定が有効であることを確認する	有	High	要	暗号化されていないので暗号化を行う。作り直しが必要	3 のRDSインスタンス	
セキュリティグループにおいて、0.0.0.0/0 からサーバ管理用ポートへのインバウンドアクセスを許可しないこと	有	High	要確認	対象のセキュリティグループはWorkspaceで使っているディレクトリのため変更や削除は出来ない。	2つのセキュリティグループ	

クラウド環境を診断した結果、CISベンチマークを基にした、BeeX独自の見解レポートをご提出。
非準拠項目を日本語で分かりやすくご説明し、改善策を伴走支援支援いたします。

BeeX × CHECK POINT™

セキュリティの状態を各セキュリティレベルのテンプレートに基づき診断
診断結果のレポーティングを実施

※診断には、Check Point社のCloud Guardを利用します。

CISベンチマークに基づいた診断・分析・改善サポート

特徴

CISベンチマークLevel2に基づき、網羅性の高い設定レビューを実施します。

想定する脅威・リスク

クラウド環境の設定ミスによる情報漏洩、インシデント対応に必要な情報の欠陥など。

おすすめのお客様

PaaSを利用するすべてのお客様におすすめです。

検査項目

- 検査基準 ： CISベンチマーク Level2
- 検査数 ： 55項目 (AWS)
  111項目 (Azure)
  64項目 (Google Cloud)

例）全IAMユーザでMFAが有効化されていること
例）rootアカウントでハードウェアMFAが有効化されていること
例）CloudTrailでログがS3に保持されること
例）CloudTrailログが適切に暗号化されていること

BeeX Propolisは最新のIntel® Xeon® プロセッサー上で稼働するAWS、Microsoft Azure、Google Cloudに対応します。

intel XEON

BeeX
株式会社BeeX
TEL:03-6260-6240 Mail:beex-marketing@beex-inc.com https://www.beex-inc.com/

202209