PRESS RELEASE
報道関係者各位

2024 年 6 月 3 日
株式会社 神戸デジタル・ラボ

クラウドの「設定不備」に起因するセキュリティ事故増加の注意喚起
― AWS 環境の「クラウドセキュリティ設定診断」を 20%OFF でご提供 ―

情報セキュリティサービス「Proactive Defense（プロアクティブディフェンス）」を提供する株式会社神戸デジタル・ラボ（兵庫県神戸市中央区、代表取締役社長 玉置慎一、以下 KDL）は、AWS 環境の設定に不備がないかを診断する「クラウドセキュリティ設定診断サービス」を、6 月 3 日より、通常価格の 20%割引（先着 5 社様限定）でご提供するキャンペーンを実施します。

■セキュリティ事故原因の上位に「設定不備」がランクイン
企業におけるクラウドサービスの利用率は上昇傾向が続いており、総務省の調査（*1）によると、クラウドサービスを「利用している」と答えた企業は全体の 7 割を超えています。また、それらの企業の約 9 割がクラウドサービス利用について「効果があった」と回答しており、今後更なる利用の増加が予測されます。

一方、独立行政法人情報処理推進機構（IPA）の発表（*2）によると、不正アクセス被害の原因のうち「設定の不備」は 2 番目に多く、同機構が毎年発表する「情報セキュリティ 10 大脅威（*3)」の組織向け脅威でも「不注意による情報漏えい等の被害」の順位が年々上昇しており、「設定不備」によるセキュリティ事故が増加傾向であることが顕著に現れています。

クラウドの「設定不備」には、データのアクセス権やストレージの公開設定に制限をかけていなかった、機密情報を暗号化できていなかったといったケースがあり、クラウドサービスをデフォルト（初期設定）のまま利用していたことがその原因となったケースもあります。

■クラウドの「設定不備」は企業経営に影響を与える問題
クラウドの「設定不備」が原因で起こり得るセキュリティ事故には、個人情報や機密情報の漏えい、ファイルの削除や改ざん、マルウェア感染、さらにはシステムの乗っ取りや停止な

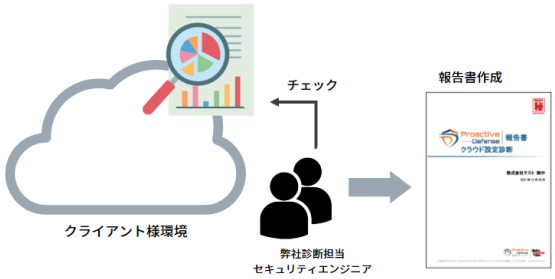
どがあります。個人情報や機密情報の漏えいは、悪意を持った攻撃者によるものだけでなく、非公開であるはずの情報が「設定不備」によって意図せず公開されてしまうケースもあります。
事故が起これば、企業の信用失墜や機会損失、事故対応のための多額の費用など、企業経営に大きな影響を与える可能性があることを理解しておくことが重要です。

■継続的な監視と設定の管理で事故を防ぐ
クラウドの「設定不備」への対策は、それだけを単独で考えるのではなく、システムを守るために必要なセキュリティ対策のひとつとして考え、セキュリティ事故を防ぐために、システムの脆弱性診断やソフトウェアのセキュリティアップデート、その他さまざまな対策を行うのと同じように、利用するクラウドプラットフォームごとに適切なセキュリティ対策を検討、実施することが必要です。
まずは現状のクラウド設定を診断し、設定をセキュア（安全）な状態にすることが求められます。さらに、次々と追加されるクラウドプラットフォームの新しい機能やルールに対応するため、継続的な監視と適切なクラウド設定の管理を行う必要があります。

特に、日本の企業で最も利用されるクラウドプラットフォーム「Amazon Web Services（AWS）」の設定においては下記が重要なポイントです。

1．アクセス管理の徹底：IAM ユーザーとロールの適切な管理
2．データの暗号化：S3 バケットや EBS ボリュームの暗号化
3．ログの管理：CloudTrail や CloudWatch Logs の有効化と監視
4．ネットワークセキュリティ：セキュリティグループや VPC の適切な設定

■KDL「クラウドセキュリティ設定診断サービス」のご紹介
KDL の情報セキュリティサービス「Proactive Defense」では、AWS 環境に設定不備がないかを診断する「クラウドセキュリティ設定診断サービス」をご提供しています。
クラウドプラットフォームが提供するセキュリティサービスによる自動診断と当社エンジニアによる手動診断を組み合わせ、CIS（*4）が提供するベストプラクティスに沿って、AWS に存在する様々なリソースの設定状況を診断、結果や修正方法をレポートにまとめてご報告します。



また、診断終了後の継続的な監視と適切なクラウド設定の管理をサポートするアドバイザリーサービス（オプション）では、「セキュリティサービスの操作方法が分からない」「新しく検出されたルールの対応方法が分からない」といった技術的なご質問に当社エンジニアがお答えします。

◎Proactive Defense「クラウドセキュリティ設定診断サービス」

対象環境：Amazon Web Services（AWS）

割引価格：26.4 万円（税抜）　◆20%割引キャンペーン実施中（先着 5 社様限定）

サービスサイト：https://www.proactivedefense.jp/services/vulnerability-assessment/cloud-security

※上記価格は 1 リージョン分の費用です。診断対象となるリソース数の上限を超えた場合は追加費用が発生します。

※CIS ベンチマーク最新版 v3.0.0 推奨設定に対応しています。

*1：総務省「情報通信白書令和 5 年度版」
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r05/html/datashu.html#f00250

*2：IPA「コンピュータウイルス・不正アクセスの届出状況（2023 年 1 月～12 月）」
https://www.ipa.go.jp/security/todokede/crack-virus/ug65p9000000nnpa-att/2023-report.pdf

*3：IPA「情報セキュリティ 10 大脅威」
https://www.ipa.go.jp/security/10threats/index.html

*4：Center for Internet Security（CIS）。米国国家安全保障局(NSA)などの政府機関と、企業、学術機関などが協力して、インターネット・セキュリティ標準化に取り組む米国の団体。

【会社概要】

会社名　：株式会社 神戸デジタル・ラボ
代表者　：代表取締役社長　玉置慎一
所在地　：〒650-0034　兵庫県神戸市中央区京町 72 番地 新クレセントビル
設立　　：1995 年 10 月
資本金　：5,000 万円
従業員数：163 名（2024 年 5 月 1 日現在）
URL　　：https://www.kdl.co.jp/

【本件に関するお問い合わせ先】
株式会社 神戸デジタル・ラボ
デジタルビジネス本部 テクニカルサービスチーム　大西翔太、深井亨
E-mail：info@proactivedefense.jp　/　電話　：078-327-2280

※テレワーク推進企業です。メールでご連絡いただけますと幸いです。
　取材など随時対応しますので、お気軽にお問い合わせください。