サイバー攻撃対策通信

令和６年８月２日
令和６年度第２号
栃木県警察本部
警備部警備第一課

クラウドセキュリティの設定、間違えていませんか？

クラウドサービスにおける**重大なインシデント**は度々発生しており、その**原因は単なる設定ミス**であることがほとんどです。

カテゴリ	発生しやすい設定ミスの概要	想定リスク
IDとアクセス管理	退職者の認証情報を失効させずに放置	ユーザー情報の悪用
	アクセスキーなどを公開のリポジトリに誤って登録	不正アクセス
	ゲストの利用者に対して誤って強力な権限を付与	情報漏洩
ロギング	ロギングの設定ができていない	インシデント発生時に影響範囲の特定ができない
	想定していたよりもログの容量が大きくなってしまう	想定以上に多額の料金を請求される
オブジェクトストレージ・データベース	適切なライフサイクル設定ができていない	保存データの喪失
	暗号化の設定ができていない	情報漏洩時にデータの内容を保護できない
	ストレージを公開設定にしてしまい、第三者に閲覧可能な状況となっていた	情報漏洩
	サービス停止と共に主なリソースは削除したが、ストレージが公開設定のまま残っていた	情報漏洩
仮想サーバ	運用中の仮想サーバを誤って削除	稼働中のサービスが意図せず停止
	不要な仮想サーバを誤って起動又は起動したまま放置する	脆弱性の放置された仮想サーバが攻撃の踏み台にされる
ネットワーク	SSH、RDP接続を許可し、のちに元に戻すのを忘れる	不正アクセス
	DNS設定手順を誤る	ドメイン名ハイジャックを受ける

出典：IPA（独立行政法人情報処理推進機構）クラウドセキュリティ～設定ミスとの付き合い方～　表：発生しやすい設定ミス

設定ミスは人間の様々な原因・理由により発生し、人間は完璧ではなくミスをしてしまうため、発生そのものを防ぐことは難しいです。
設定ミス自体の発生を完全に防ぐというのではなく、設定ミスは発生するものとして許容し、インシデントに繋がらないように是正していくという心構えが大切です。

TPCCAT
Tochigi Police Counter Cyber Attack Team

参照：IPA（独立行政法人情報処理推進機構）HP　クラウドセキュリティ～設定ミスとの付き合い方～
https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2023/cloud-security.html
⇒クラウドにおけるセキュリティの考え方の詳細が掲載されている。