監査に合格しても情報漏洩は止まらない
定期的なセキュリティ評価こそ重要

EQUIFAX　Marriott HOTELS · RESORTS · SUITES　BRITISH AIRWAYS

企業の情報漏洩が止まらない

- **Equifax -**Equifaxは、Ernst & Young (E & Y) のCertifyPointによるISO 27001認定を受けていた。だが、政府の取締官によって、ごく基本的な制御が行われていないことが発見された結果、4億5,000万ドルの和解金を支払うことになる見通し。
- **Marriott (Starwood Hotels)** の被害: 2014 -2018 パスポート番号を含む**5**億件の情報漏洩。 **Marriott** は2020年3月にも520万人の宿泊客情報漏洩が発覚。今回の漏洩で多要素認証による対策が強く求められています。
- **British Airways** の被害: 8/21/2018 –9/5/2018 **500,000**件近い情報が流出。GDPRによる罰金は推定2億8,000万ドル。

更なる規制強化

GDPRの次にCCPAがやってくる

- カリフォルニア州消費者プライバシー法（CCPA）は、カリフォルニア州の住民のためのプライバシー権と消費者保護を促進する法律で、2020年1月1日に施行。海外と取引のある日本企業にも影響の懸念。

考えうる政府機関による罰金

- カリフォルニア州消費者プライバシー法に故意に違反した場合、**1件当たり7,500ドル**未満の制裁金を課されることになる。尚、このプライバシー法はカリフォルニアだけでなく、全ての州で施行され出しています。

内部犯罪の脅威ーヒツジの皮をかぶった狼

- 企業のハッキングのうち平均35%が、社内の既知ユーザによるものだった。
- 情報を**1**度引き出せばよいだけ。

最近のセキュリティ監査からの話題

過去の権限設定がそのまま有効

- RACF導入当初に設定した高権限が今でも有効に機能しており、必要以上の権限付与を見直すよう監査から求められる。導入当初の高権限が時間の経過と共に忘れられ、環境の変化に追従せず現在でも有効のまま残っている。

サロゲート機能利用が問題視

- 本来行ってはいけないRACF設定業務を、権限管轄外のユーザーによって実施されていたことが外部監査で発覚し、定期的な監査情報提供が要求された。管理者権限を利用できるサロゲート機能は運用管理で良く利用されている落とし穴。

IMPACT

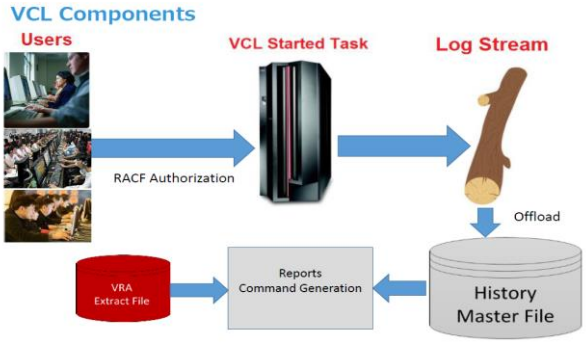
最新のアクセス状況をモニターして記録

過度のアクセス権限を見直す

- 定期的な棚卸作業で不要な定義は整理されていると思いがちですが、調査に時間を要する作業は先送りされることが多く、セキュリティ監査によってRACF稼動当初に定義したアクセス権限が今でも残っていて、現在でも使われている例が多数発見されています。過度のアクセス権限を見直すため、必要なデータのみを収集するためにモニターを開始する必要があります。

サロゲート利用状況の把握も重要

- 高権限の責任者IDを使ってアクセスするサロゲート機能は運用に便利な機能なので広く利用されていますが、管理権限外の作業有無を把握するため、サロゲート(代理) 機能を利用して、誰が、いつ、どのユーザー権限を利用してアクセスしたかを確認することが極めて重要です。特に、アウトソースしている場合、依頼元の管理責任が問われることになります。



安全にアクセス権限変更

未使用定義を抽出して削除

- モニターデータを利用して退職者IDなど一定期間未使用であった定義削除やアクセス権限変更のRACFコマンドを生成します。SMFデータからは未使用情報を抽出することができません。

影響分析後に本番システムの権限変更

- 生成したRACFコマンド適用前に影響分析レポートによる確認やモニターデータを利用したシミュレーションで安全であることを事前に検証した後、本番システムに適用します。

ベースライン設定で改善進捗状況を把握

アクセス権限見直し修正後ベースライン設定した運用へ

- アクセス権限を見直し修正することで正しいアクセス定義のベースラインが完成し、定期的な見直しと改善を実施することで安全で健全な運用管理を実現できます。

Vanguardツールの有効性

- Vanguardツールは、モニターデータ収集からRACFコマンド生成、シミュレーションによる影響分析レポートなどの一連の運用業務を強力にサポートします。

(No.カ-AI-01-02)

総販売元

株式会社ブロード

東京：〒100-0014　東京都千代田区永田町1-11-30
TEL（代表）：03-6205-7463

Email：broad@broad-corp.co.jp
URL：http://www.broad-corp.co.jp