

DBセキュリティ監視サービス - 今、データベースそのものが狙われています -

相次ぐDBからの重要情報流出被害

◆金融関係A社

内部から顧客情報148万人分の顧客情報が流出
 <影響>
 ・社会的信用の失墜
 ・多大な損失額:お詫びとして5万人に1万円送付

◆音響機器販売B社

外部からの不正侵入による9万7千人分の個人情報漏洩
 <影響>
 ・約1ヶ月超のクレジット通販業務の停止
 ・高額な調査費用、顧客への賠償費用
 ・顧客の信頼度低下

問題点 -DBの観点から-

DBへの不正アクセスを見抜けなかった

原因

DBへのアクセスログを取得してない

DBへの不正アクセスが定義されていない

DBへのアクセスログを分析・評価できていない

解決案

- ・不正アクセスログ取得
- ・不正アクセスを発見する仕組み
- ・監視導入時に既存環境へ変更を加えたくない



- ・高性能／高機能なDB監視装置
- ・高精度な監視ポリシー設計スキル、アラート判定スキル



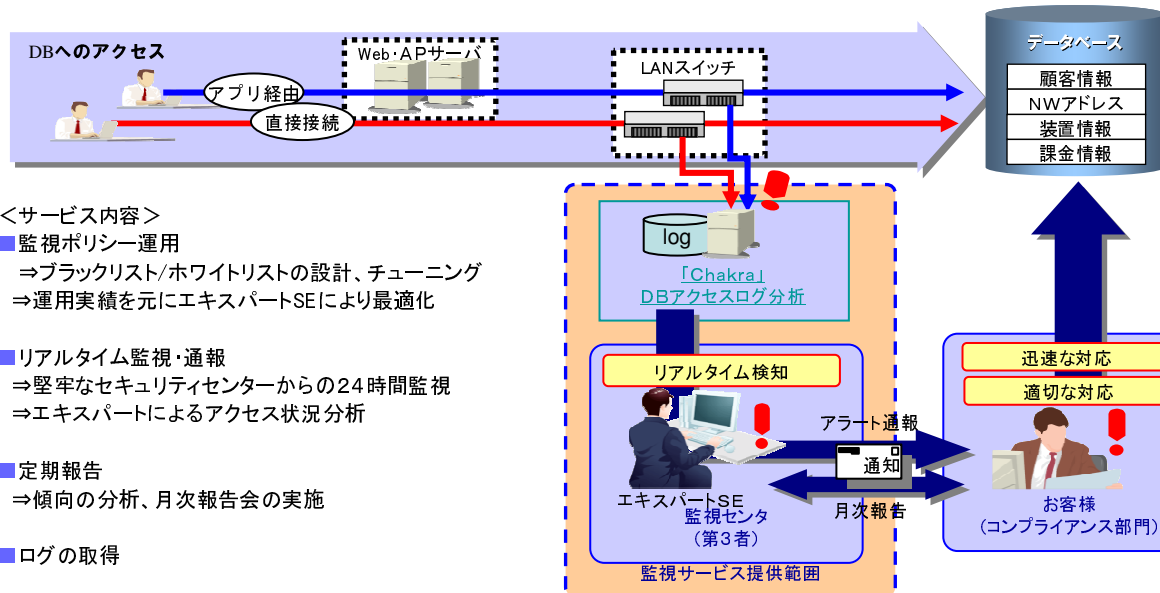
効果として・・・

- ・不正アクセス早期発見
- ・不正アクセス抑止
- ・事故時の追跡調査、および正当性の証明が可能

DBセキュリティ監視サービス

既存システムに影響なく、DBアクセスログを早期に取得開始

リモート監査により、リアルタイムに不正アクセスを発見



<サービス内容>

- 監視ポリシー運用
 ⇒ ブラックリスト/ホワイトリストの設計、チューニング
 ⇒ 運用実績を元にエキスパートSEにより最適化
- リアルタイム監視・通報
 ⇒ 堅牢なセキュリティセンターからの24時間監視
 ⇒ エキスパートによるアクセス状況分析
- 定期報告
 ⇒ 傾向の分析、月次報告会の実施
- ログの取得

【お問い合わせ先】 株式会社 富士通九州システムズ (FJQS)

東京オフィス 〒144-0035 東京都大田区南蒲田2-16-2 テクノポート三井生命ビル9F

Tel. 03-5703-7028 Fax. 03-5703-7050 (担当:セキュリティセンター)

大分事業所 〒870-8551 大分県大分市東春日町17-58 (ソフトパーク内)

Tel. 097-534-8119 Fax. 097-535-1064

2009. 6