ケース分析: DoCoMo – JavaScript

- 発生日: 2009年5月22日
- 症状

  DoCoMoの携帯電話に組み込まれたJavaScriptが本来はアクセスできないWEBサイトにもアクセスできるようになってしまった。

  DoCoMoは当該携帯電話の販売を一時中断した。
- 原因

  JavaScript処理系の実装にバグが原因だった。

  SOP (Same Origin Policy)セキュリティポリシーの実装に問題があった。DoCoMo発行の仕様書に不明瞭な記述があり、製造者が間違って解釈して実装した。
- どのシステム機能があったらこの障害の影響を最小化できたか？
  - 許可されてないアクセスをブロックする機能。
  - JavaScript処理系を切り離し他の処理を継続する機能。

ケース分析: Google Apps – Gmail

- 発生日: 2009年2月24日
- 症状

  Google Apps Gmail利用者が自分のアカウントにアクセスできなくなった。
- 原因

  データセンターでの通常のメンテナンス作業中に想定外のサービス中断が起きた。このようなデータセンターでの障害の際には、利用者からのリクエストは代替のデータセンターに転送されるようになっている。しかし、利用者データを最適化するために導入した新しいソフトウェアの予想外の副作用によりGmailの潜在的バグにヒットした。結果、代替データセンターが過負荷に陥り、それが引き金となり複数に他のデータセンターの過負荷を招き障害に至った。
- どのシステム機能があったらこの障害の影響を最小化できたか？
  - 障害の原因を同定するエビデンスの記録と提示機能。
  - タイムシフトリハーサルの機能。
  - 新しいソフトウェアの導入を取り消す機能。
  - 過負荷状態を避けるための資源制限機能。

ケース分析: ANAチェックインシステム

- 発生日: 2008年9月14日
- 症状

  複数空港でのチェックイン端末が早朝から操作不能になった。
- 原因

  端末からサーバーシステムにアクセスする際の証明書の有効期限が前日で切れていたためにアクセス出来なくなっていた。
- どのシステム機能があったらこの障害の影響を最小化できたか？
  - 原因を同定するエビデンスの記録と提示機能。
  - タイムシフトリハーサルの機能。
  - サービスを継続することを優先するようなセキュリティ制御機能。
  - 障害の予兆を検出するプロアクティブな管理機能。

ケース分析: 東京証券取引所

- 発生日: July 22, 2008
- 症状

  証券取引所のデリバティブのトレーディングシステムが利用できなくなった。
- 原因

  1つの記述子の作業領域の大きさが想定より大きく小さく定義されていた。その為、複数の記述子を格納できなくなり情報ロスにつながり障害が発生した。
- どのシステム機能があったらこの障害の影響を最小化できたか？
  - 当該処理を切り離して、他の処理を継続する機能。
  - 障害の予兆を検出するプロアクティブな管理機能。
  - ソフトウェアの老化による障害につながる前にソフトウェアを若化する機能。

ケース分析: 日本シグナル (Suica改札機)

- 発生日: 2007年10月12日
- 症状

  東京エリアのSuicaカード利用の改札機が動作しなくなった。

  JR東日本は改札ゲートを開放した。
- 原因

  新サービスの導入のための構成変更が行われた結果、サーバから改札機に無効リストを送る際の大きなデータを分割送信する処理に不具合が発現し、再試行処理が無限に繰り返されるようになってしまった。
- どのシステム機能があったらこの障害の影響を最小化できたか？
  - 新サービスに対応するための構成変更に対応出来る機能。
  - タイムシフトリハーサルの機能。
  - ソフトウェアの老化による障害につながる前にソフトウェアを若化する機能。
  - 障害部位を隔離し全体障害を避ける機能。
  - 原因を同定するエビデンスの記録と提示機能。
  - 新サービスの導入を導入前に戻す機能。

ケース分析: NTT IP電話システム

- 発生日: 2006年9月19日、2006年10月23日、2007年5月16日、2007年5月23日
- 症状
  - IP電話が不通になった。
  - NTT東日本とNTT西日本間の接続が不通になった。
  - フレッツサービスが7時間にわたって利用できなくなった。
- 原因
  - シグナリングサーバのバグにより処理が過負荷になった。
  - 負荷計画時の見積もりが甘かったためシグナリング処理が過負荷になった。
  - システムメンテナンス時に間違ったデータがリストアされた。
    結果、シグナリングサーバが停止した。
  - 1つのルータが故障し、間違ったルーティング情報が伝搬した。
    ルータの再起動での回復が確実に見込めなかったので対応が遅れた。
- どのシステム機能があったらこの障害の影響を最小化できたか？
  - 障害のあった部位を切り離し、全体の停止を防ぐ機能。
  - 資源利用に制限を設ける機能。
  - 操作を元に戻す機能。
  - 原因を同定するエビデンスの記録と提示機能。

ケース分析: ANA発券システム

- 発生日: May 27, 2007
- 症状

  ANA発券およびチェックインシステムが停止し、

  130便がキャンセルになり306便が遅れた。
- 原因

  ネットワーク機器のハードウェア故障によりホストコンピュータと端末間の通信に輻輳が起こった。それらの因果関係は不明。
- どのシステム機能があったらこの障害の影響を最小化できたか？
  - 障害の原因を同定できるエビデンスの記録と提示機能。
  - 利用される資源を制限する機能。
  - 障害部位を切り離し、全体の停止を防ぐ機能。
  - 障害を予知するプロアクティブな管理機能。

ケース分析: 航空管制

- 発生日: March 1, 2003
- 症状

  FDP (Flight plan Data Processing) システムが停止し、
  215便がキャンセルに、1500便に遅れが出た。
- 問題

  特定のメモリアドレスをアクセスしてことで潜在バグが発火した。
  テスト不足が原因だった。
- どのシステム機能があったらこの障害の影響を最小化できたか？
  - APIの範囲チェック機能。
  - 操作を元に戻す機能。
  - タイムシフトリハーサルの機能。
  - ソフトウェアの老化による障害を避けるための若化機能。