Engineer

インシデント対応

⏏ 障害やセキュリティー事故に対して判断と対処を調整すること

どのようなものか

インシデント対応とは、サービスが中断したり、システムに重大な脅威が見つかったりしたときに、対処を調整して進めることです。インシデントは対応が必要になった事態そのものです。対応には、問題の検知と宣言、作業の分担、利用できる状態への復旧、残る作業の引き継ぎが含まれます。開発や運用の担当者に加え、利用者を支援する人も関わります。事態によっては、セキュリティーや法務の判断を任された人が必要になります。

NISTが示すサイバーセキュリティーのインシデント対応指針では、検知、対応、復旧を、準備と継続的な改善が支えます。この指針の対象はサイバーセキュリティーです。役割を割り振り、判断を記録する考え方は、リリース後の障害にも応用できます。データが外部に出た可能性があるときは、サービスが動いていても、証拠の保全や利用者の保護が必要になることがあります。一般的な障害では、問題のある経路を避け、安全に利用を再開できるようにすることが先かもしれません。

Googleのインシデント管理の解説では、対応全体を見る指揮役、運用上の処置を取りまとめる人、連絡を担当する人を分けています。初動では一人がいくつかを兼ねることがあります。参加者が増えたら、各役割の担当者を明記すると、同じ調査を二人で行ったり、異なる指示が出たりするのを防げます。役割の組み合わせはチームの規模と状況に合わせられます。

概念を判断に生かす

「インシデント対応とは？」を実際の判断に生かしましょう。その概念を、開発または購入するシステムに結び付けて考えるお手伝いをします。 障害が小さいうちに知らせる監視とアラートを整え、安定した状態をどれだけ維持できているかを数値で示します。

サービスを見る お問い合わせ →

用語の背後にある前提を検証する

解説とリンク先の実績を参考に、プロジェクトについての質問を整理してください。ツールを選ぶ前に、前提を一緒に検討できます。 社内初のオブザーバビリティダッシュボードを構築 — 社内システムの状態を初めて可視化

社内初のオブザーバビリティダッシュボードを構築 お問い合わせ →

なぜ重要なのか

対応の初めには、情報の確かさがそろいません。計測値から決済の失敗が増えたことはすぐ分かっても、どの利用者や支払い方法に影響があるかは、時間をかけて確かめる必要があります。利用者からの申告を受ける窓口が、先に傾向をつかむこともあります。共有する時系列には、観察した内容とその出どころ、どこまで確かかを書きます。後から参加した人は、最初に出た仮説を事実として扱うことなく調べられます。

作業を調整すれば、急いで加える変更のリスクも抑えられます。以前の版に戻すことと、設定を一時的に変更することは、個別には妥当でも、同時に行うと互いの効果を損ねる場合があります。運用をまとめる人は、何をいつ変えるか、結果がいつ見えるか、取り消しは可能かを把握します。個々の担当者は専門知識を生かして提案でき、チームは誰が決めるかを確認できます。

復旧と原因調査には別々の時間がかかります。トラフィックを別の経路へ移せば、原因が分かる前にサービスが使えるようになる場合があります。復旧の判断には、新しい注文が完了し、保留中の注文の照合が進んでいる、といった条件を定めます。その後の振り返りでは、なぜ障害が起きたか、対応はどう機能したか、何を変えるべきかを見ます。対応中の判断や検証を残しておけば、後から根拠をたどれます。

実際の活用例

予約サービスがときどき支払いを受け付ける一方で、チケットを発行しないとします。窓口に最初の連絡が入り、開発担当者が失敗した要求を確認しました。最初に対応した人はインシデントを宣言し、症状を確認した時刻を書きます。チームで分かっている影響を短くまとめ、変更を取りまとめる人を決めます。窓口には連絡先と次の更新時刻を伝えます。

運用担当者は影響を受けた予約をいくつか調べ、開始時刻と重なる最近の変更を見つけます。指揮役は、以前の版へ戻しても、決済済みの記録が確認できることを先に確かめるよう頼みます。一人が切り戻し、別の人が決済とチケット発行の様子を見ます。窓口は未解決の予約番号を保管し、確定していない予約について、利用者が取れる安全な行動を知らせます。

復旧を確かめるには、一つの支払いに正しいチケットが対応するところまで確認します。保留中の予約がどの程度処理されたかも見ます。再び使えるようになった時刻と、残る予約を誰が照合するかを記録します。通常の運用で残るリスクを扱えるようになれば、対応を終了できます。原因調査には別の担当と期限を決めます。交代のときは、直近の確定事項と進行中の操作、次の連絡時刻を引き継ぎます。

Engineerのmacosアプリで増え続けるメモリー消費に対処した事例には、別々の測定と、保持するイベントを制限した作業が記録されています。測定がどこまでの状況を示すかを残す大切さが分かります。予約サービスは、作業と連絡をどう調整できるかを示す架空の例です。

問題が起きるところ

確実になるまで宣言を待つ。 影響がありそうなら、担当者と次の確認時刻を決めて調べられます。人を集める条件を普段から決めます。追加の情報で深刻でないと分かれば、体制を縮小できます。

複数の人が同時にシステムを変える。 予定や実施した作業を、担当者とともに共有します。可能なら、次の変更の前に一つ目の結果を確かめます。独立に進められるものは範囲を明らかにします。

推測が利用者に伝わる。 何が起きているか、何をしてよいか、いつ次の情報が出るかを伝えます。不明な点は不明と明記し、原因の説明には確認できた情報を使います。

復旧した時点で残りの作業が見えなくなる。 予約の照合、利用者への連絡、一時的な対策の見直しを担当者に割り当てます。対応の連絡先を閉じる前に、通常の作業管理へ移します。

参考資料

- NIST SP 800-61改訂第3版 — サイバーセキュリティーのインシデント対応と、その準備・改善。
- Googleによるインシデント管理の解説 — 対応時の役割分担、連絡、記録。
- Google SREワークブックのインシデント対応 — 具体的な対応の例と教訓。

用語集

実際の制約に合わせて選ぶ

デプロイの流れ、運用上のリスク、緊急対応の担当者をお知らせください。検査、復旧手段、明確な責任の所在を伴う変更の範囲を定められます。

料金を見る お問い合わせ →

用語を実務に結び付ける

「インシデント対応とは？」がお客様の組織にどう当てはまるかをご相談ください。現在のシステムの具体例が一つあれば、話を始められます。

サービスを見る

welcome@engineer.company +45 50 10 61 84 デンマーク、コペンハーゲン

このページを持ち歩く

連絡先カード

心を込めて丁寧に制作： D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

著作権 © 2025 – 現在 · Engineer ApS · すべての権利を留保します。

印刷元： https://engineer.company/ja/glossary/incident-response/