Engineer

インシデント

システムのデータやサービスを危険にさらす出来事

どのようなものか

インシデントは、稼働中のシステムの問題が、予定の仕事を中断し、今すぐ対応する必要があるほど深刻になったものです。応答しなくなったサービス、改変された記録、メモリーを使い切ったマシン、他人が使っているアカウントなどです。セキュリティチームは「セキュリティインシデント」、運用チームは「本番インシデント」や単に「障害」と呼び、大半の組織は重大度のレベル別に分類します。

NISTのインシデント対応指針は、三段階で区別し、セキュリティ以外にもよく当てはまります。イベントは、ログインの試行、ソフトウェア更新、アプリの応答など、コンピューティング資産に関わる、観測できるあらゆる出来事です。有害な事象は、原因を問わず悪影響があるもので、指針は、攻撃と並べて、自然災害や停電も挙げます。インシデントは、組織の基準を満たすと、誰かが判断した有害な事象です。指針は、その判断に「宣言する」という動詞を使います。基とする米国連邦法の定義は、情報やシステムの機密性、完全性、可用性を、現実に、または差し迫って脅かす出来事、あるいはセキュリティポリシーへの違反を含みます。

セキュリティと運用では、この言葉の重心が違います。前者では、通常、敵対者、ポリシー違反、外部へ出た可能性のあるデータを意味します。後者では、攻撃者が登場しなくても、予定外の中断や、サービスの深刻な劣化を指します。語彙から想像する以上に、両者は重なります。サービス拒否攻撃と通常のアクセス急増は、初めはグラフ上で似て見えることがあり、満杯のディスクも、侵入者と同じほど、徹底してデータを失わせ得ます。

近い言葉も、区別する必要があります。欠陥は、製品の不備です。何年も気付かれずに存在し、害が出て初めて、インシデントの一部になります。アラートは、何かがおかしいかもしれないと知らせるメッセージです。インシデントにならな

いものも多く、逆に顧客が最初に報告するインシデントも多くあります。サービス管理では、一件以上のインシデントの背後の原因を、「問題」として別に追跡します。

概念を判断に生かす

「インシデントとは？」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

この言葉の中にある決定は、しきい値です。遅いページ、不審なログイン、増えるキューが、どこから、一人の技術者のチケットではなく、チームの最優先になるのでしょうか。高すぎれば、広がる侵害を、その拡大が見えない担当者が、通常業務として扱います。低すぎれば、何度も仕事から呼び戻され、宣言の意味がなくなります。NISTの答えは、必要になる前に、基準に合意することです。既知の誤検知も考慮し、有害な事象が、組織の定義済みの基準を満たせば宣言します。例付きで書いた基準は、午前二時の口論より、はるかに安く済みます。

宣言は、誰が何をするかを変えます。一人は、デバッグするのではなく、指揮と調整を担い、ほかの人は通常業務から離れ、一つの連絡経路へ事実を集め、時刻付きの記録を始めます。そうしなければ、同じ人たちが同じ仕事を並行して行い、問題を最初に明確に述べるのが、顧客の文章になります。

一部の会社では、法的な時計も動きます。EUのNIS2指令、Directive (EU) 2022/2555は、対象組織に、重大なインシデントを国の当局へ報告するよう求めます。認識してから24時間以内に早期警告、72時間以内にインシデント通知、その通知から一か月以内に最終報告です。定義は、攻撃だけでなく、ネットワークと情報システムが提供するデータやサービスの、可用性、真正性、完全性、機密性を損なうあらゆる出来事へ及ぶため、深刻な停止も該当し得ます。二日目になって「これはインシデントか」と問い始めるチームは、すでに最初の期限を使い切っています。

運用費用は人の時間で、以前より増えています。NIST指針の2025年改訂は、今では頻繁に起き、復旧にはしばしば数週間や数か月かかると記します。2012年の前版は、まれに起き、一、二日で終わると想定していました。インシデントの

予算には、その夜だけでなく、後続作業も含めます。

実際の活用例

このサイトで紹介する一件は、macOSのデスクトップアプリに関するものです。診断レポートは、36 GBのマシンで、圧縮ページ111 GBを記録しました。日付は2026-09-01です。別のメモリー使用量サンプルは、アプリのコアのイベントを出す接続再試行ループ中に、毎秒約41 MBの増加を記録しました。調査は、上限のない主ストリームがログイベントを保持し、そのログイベントを使わない購読側へもコピーすると突き止めました。バッファーに上限を設け、イベント種別で購読を絞り、ログの単位時間当たりの出力量に予算を与えました。全テスト実行の比較では、アプリのコアのログ行が610,996行から1,411行へ減りました。この測定は、テスト実行のものであり、本番通信や修正後のメモリーではありません。アーキテクチャの検査とアプリの予算テストで、上限を設けた設計を守ります。あふれた際の方針では、繰り返す診断を捨て、影響を受けた状態を更新し得ます。終了処理のタイムアウトには、別途修正が必要でした。

繰り返すインシデントもあります。Google CloudとLinuxシステム間の八つのWireGuard、IPsecトンネルは、不安定で診断が遅く、一本の停止で、環境間の通信が切れ得ました。設定を標準化し、正常性を監視し、再起動する代わりに、繰り返す経路制御や鍵交換の問題を、根本から解消しました。繰り返す接続インシデントは止まりました。同じことが三度起きるなら、対処すべきインシデントは、原因そのものです。

誰かが手伝おうとして始まるものもあります。管理ツールのない基盤では、所有権に関する申請の承認、レビューの非表示、キャッシュの消去を、データベースコンソールを持つ技術者が行います。事例は、それを遅く、記録がなく、入力ミス一つでインシデントになる方法と呼びます。そこで構築した、128の部品からなる、約40の管理経路を持つ運用バックオフィスは、製品のほかの部分と同じ認可と監査証跡の下へ仕事を移します。その代わり、大きな内部機能群のテストとアクセシビリティを維持する費用が、続きます。

問題が起きるところ

五人が対応し、指揮する人がいません。 チャットが仮説で埋まり、二人の技術者が別々のものをロールバックし、顧客には一時間何も届きません。誰も宣言せず、調整役を任命しなかったためです。チームの誰でも宣言できるようにし、最初に、全体像と記録を保つ責任者一人を決めます。

同じインシデントが、数週間ごとに戻ります。 サービスが戻れば対応を終え、再起動を修正と数えます。サービスの復旧と原因の除去を、二つの仕事とし、前者はその夜に閉じ、誰かが寝床へ戻る前に、後者の担当者と期限を決めます。

ツールが、インシデントを大きくします。 イベントごとに一行書くログは、障害と同じほど大きくなり、警報規則は、一つの原因へ何百もの通知を送ります。事前にログと警報の出力量を決め、繰り返しをまとめ、報告する障害自体の負荷の下で、報告経路を試験します。

修正が、次のインシデントを起こします。 本番へ急いで手入力した変更が、一つの症状を直し、別の問題を始め、後の検証に必要な時系列記録へ穴を残します。証跡の残る、事前承認済みの短い復旧操作一覧を用意し、対応中の変更をすべて記録します。

教訓が、数か月遅れて届くか、責任追及になります。 数週間の復旧後に検証しても、覚えていることはわずかです。誰が間違えたかを問う検証では、人は次の間違いを隠すようになります。NISTの改訂指針は、多くの場合、見つけたらすぐ教訓を共有するべきとし、復旧指針の最後に、インシデント、対応、学んだことの事後報告を置きます。間違えやすくした条件を書き、それを変えます。

参考資料

- インシデント — NIST文書の各定義と、その基になる法律や標準です。
- SP 800-61 Rev. 3 — 単一の対応サイクルではなく、CSF 2.0の機能に沿って構成した、NISTの2025年の対応勧告です。
- Cybersecurity Framework — 指針が対応付ける、Govern（統治）、Identify（特定）、Protect（防御）、Detect（検知）、Respond（対応）、Recover（復旧）の機能を持つ枠組みです。
- RFC 2350：コンピューターセキュリティインシデント対応への期待 — 対応チームが自分自身について公開するべき内容に関する、IETFの現行ベストプラクティスです。

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/