Engineer

情報セキュリティ

データとシステムを不正利用や被害から守る取り組み

どのようなものか

情報セキュリティは、情報と、それを保存・伝送するシステムを、所有者が意図した状態に保つための取り組みです。読むべき人だけが読み、意図した方法でだけ変更され、必要なときに使える状態を保ちます。日常の会話や多くの職名では、単にセキュリティと呼びます。NISTの用語集にある定義は、米国の連邦法44 U.S.C. 3552に由来し、三つの特性を挙げています。機密性は、アクセスと開示に対する正当な制限を維持することです。完全性は、不適切な変更や破壊から守ることであり、情報が真正なものであると示せることや、送信者が「送っていない」と主張しても、その主張が成り立たないと示せることも含みます。可用性は、情報に適時かつ確実にアクセスし、利用できることです。

この三つは互いに相反し、その緊張関係が作業を難しくする主な理由です。誰も接続できないデータベースは、機密性が完全でも、誰の役にも立ちません。3か所に保管したバックアップは可用性を高めますが、盗もうとする人にも探す場所を3か所与えます。この分野の判断の多くは、ある種類の情報について、相反する要請のどこに折り合いを付けるかというものです。公開価格表と患者の診療記録とでは、答えは大きく異なります。

具体的な作業は、それぞれ明確な目的を持つ保護手段である管理策を通じて行います。暗号化、認証、ファイアウォール、アクセス制御など、技術的なものがあります。変更の公開前レビュー、退職者のアクセス権を最終日に解除する規則、文書化されたインシデント対応計画など、手続き上のものもあります。施錠された部屋のように、物理的なものもあります。NIST SP 800-53は、このような管理策を分類したカタログであり、組織が自らのリスクに合うものを選べるように書かれています。NIST Cybersecurity Framework 2.0は、一段上の水準を扱います。「統治」「識別」「防御」「検知」「対応」「復旧」という六つの機能の下に達成すべき結果を示し、その達成方法を規定するものではないと明記しています。

概念を判断に生かす

「情報セキュリティとは？」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。 アカウント、パスワード、権限を整理し、業務に必要なアクセスだけを付与し、退職者の権限は当日に解除します。

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。 Linuxサーバーを守る1,000件のRBACルールを作成 — 1,000 セキュリティ上の穴を塞ぐアクセスルール

Linuxサーバーを守る1,000件のRBACルールを作成 お問い合わせ →

なぜ重要なのか

情報に生じた損害は、元に戻すのが困難です。漏えいしたデータは、その後で何を修正しても、漏えいしたままです。気付かれずに改ざんされた記録は、それを根拠に後から行ったすべての判断を疑わしいものにします。給与計算の日や入札締め切り日に起きる停止は、停止時間そのものを超える損失をもたらします。通常、まずその情報の当事者に、次いで保有していた会社に負担が及びます。

発注者にとって難しいのは、セキュリティが機能している間は、その働きが見えないことです。二社の提供事業者が同じツールを同じ言葉で並べていても、一覧どおりに機能することを確認したのは一方だけかもしれません。したがって、役立つ質問は証拠についてのものです。どの管理策が導入されているか、導入した日ではなく今日も機能しているとどう確かめているか、どれかが問題を報告したら何が起きるかを問います。稼働中のシステムから生成した報告書で答える事業者は、方針文書で答える事業者とは、示せる根拠が異なります。

トレードオフは現実にあり、その大半は時間や手間に関わります。すべてのスキャナーは指摘を出し、その一つ一つについて、人が重要かどうか判断する必要があります。ログインの手順を増やすたびに、人はそれを避ける方法を探します。追加した管理策はすべて保守しなければ、気付かないうちに書類上だけの対策になります。フレームワークの先頭に「統治」があるのは、これらが技術的判断と同じくらい経営上の判断でもあるためです。誰かが、どこまでのリスクを許容するか、どのデータに最も注意を払うべきか、残りの保護にいくらかかるかを決めなければなりません。

実際の活用例

あるアプリケーションプラットフォームでは、継続的なセキュリティ検査プログラムによって、セキュリティの状態を見解ではなくビルド結果として示せるようになりました。静的解析にはCodeQL、動的テストにはZAPを使い、Goの依存関係はgovulncheckで検査します。ビルドのたびにAnchoreとSyftでソフトウェア部

品表を生成し、Gitleaksで履歴中の認証情報を探します。ビルド自体のサプライチェーンも対象です。ワークフローが呼び出す外部のActionsは、誰かが付け替えられるタグではなく、正確なコミットに固定しています。Dependabotは6つのエコシステムを監視しています。自動化と並んで、脅威モデルやOWASPのテストガイドに照らした評価を含む、21件のセキュリティ監査文書もあります。設定した検査が認識した脆弱性によって、ビルドを失敗させられます。その代償は指摘の量であり、出力を有用な状態に保つには、継続的な選別と優先順位付けが必要です。

自社ホストのメモリーは464 MBで、メトリクス基盤を動かすには足りないため、代わりに稼働中のホストをMarkdownにまとめる七つの読み取り専用ロールで、セキュリティの状態を記述しています。アクセス報告は、アカウント、sudoの権限範囲、鍵のフィンガープリント、フォージの利用者、データベースのロールを扱います。セキュリティ報告は、ハードニングが設定されているだけでなく、実際に適用されているかを示します。ファイアウォールのルールを照合順に並べ、稼働中の遮断ルール集合も出力します。実行時に測定していない数値は一つも出しません。報告によって、機能していない二つのセキュリティ管理策や、宣言されていない待ち受けポートなどが見つかりました。

設定と実際の適用との差は、同じホストですでに表れていました。レート制限ルールが、先に一致する、より広いファイアウォールルールの下に1年間置かれていたため、どのパケットもその制限ルールまで到達していませんでした。現在の検査は、番号付きルール一覧と稼働中のフィルターチェーンを読み取り、順序を検証します。各ポートのルールは厳密に一つで、必ずプロトコルを指定します。SSHポートにはレート制限を設定し、許可ルールを併置しません。また、公開すると宣言した五つのポートを、集合全体として検証します。

問題が起きるところ

管理策を設定しても、実際には適用されていません。 ファイルの設定、一覧内のルール、Wiki上の方針は、誰かの意図を記録したものです。何が実際に有効かを示せるのは、稼働中のシステムに対する検査だけです。管理策をテストせず数えるだけの取り組みでは、穴が開いたまま全面的な対応を報告し、最初の本当のテストは他の誰かが行うことになります。

すべてを一つの層に頼ります。 境界の防御が強固でも、その内側のアクセスが無制限なら、一つのミスですべてを明け渡します。多層防御は、各層がいつか破られると想定し、その背後に次の層を置きます。盗まれたパスワードにも第2要素が立ちはだかり、侵害されたサービスにも、権限を絞ったデータベースロールが立ちはだかるようにします。

読める量を超えて指摘が届きます。 起こり得るすべての問題をスキャナーが同じ緊急度で報告すると、人は次第に出力を読まなくなります。担当者を明確にし、深刻度の基準を定め、どの指摘でリリースを止めるかを文書化することで、出力を読む価値のあるものに保てます。

停止して初めて可用性を思い出します。 漏えいはニュースになるため、関心の大半が機密性に向きます。一度も復元したことのないバックアップ、代替の計画がない単一サーバー、気付かないうちに期限切れになる証明書は、いずれも三つ目の特性を満たさず、その問題は最悪のタイミングで表れがちです。

外部の人にとって、問題の報告先が分かりません。 公開サービスの弱点を見つけた人には、報告先が必要です。RFC 9116は、/.well-known/security.txtから配信するsecurity.txtファイルを定義しています。報告先を示すContactフィールドと、そのファイルをいつまで信頼できるかを示すExpiresフィールドが必須です。それがなければ、報告は一般の受信箱や、最初に返答した誰かに届くことになります。

参考資料

- NIST CSRC用語集の情報セキュリティ — FIPS 200と44 U.S.C. 3552に基づく、三つの特性を伴う定義です。
- 44 U.S.C. 3552 — 機密性、完全性、可用性を定義する法律です。
- NIST SP 800-53 Rev. 5 — 分類別に整理した、セキュリティとプライバシーの管理策カタログです。
- NIST Cybersecurity Framework 2.0 — 統治から復旧まで、セキュリティ上の成果を記述する六つの機能を説明しています。
- RFC 9116 — 脆弱性の報告先を調査者に伝えるsecurity.txtの形式です。

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

「情報セキュリティとは？」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/security/