Engineer

ゼロトラスト

ネットワーク上の場所だけでは信頼を与えないセキュリティモデル

どのようなものか

ゼロトラストは、ネットワーク上の場所を理由に信頼を与えないセキュリティモデルです。2020年にこのモデルを示した米国連邦政府の文書NIST SP 800-207は、暗黙の信頼を一切与えず、継続的に評価するという前提で、リソースの保護に焦点を当てる考え方と定義しています。オフィスのネットワーク内、VPN上、同じデータセンター内にいるだけでは、リクエストに何の権限も生まれません。リソースへの要求ごとに、誰が、どの端末から、何を、どの条件で求めているかを判断します。英語でハイフンを入れたzero-trustは、zero-trust designのように名詞を修飾します。このモデルを実現する設計は、zero trust architecture、略してZTAと呼びます。

NISTは、登場する役割を正確に名付けています。主体とは、要求する人やもので、利用者、サービス、端末が該当します。リソースは、保護する価値のあるものすべてで、文書はデータのほかに、プリンターや計算能力も挙げています。その間には、3つの論理的な構成要素があります。ポリシーエンジンは、要求を許可するか決め、その判断を記録します。ポリシー管理機能は、その判断を実行し、主体とリソースの間の経路を開閉し、その1セッション用の認証情報やトークンを発行します。ポリシー適用点は、経路そのものに置かれ、セッションを通し、監視し、指示されると終了させます。

文書は、この変化を空港に例えて説明しています。乗客は保安検査を1回通ると、その先では旅行者、乗務員、空港職員がターミナルを行き交い、全員が信頼されます。このターミナルをNISTは、最後に通った検査地点の水準まで全員を信頼する「暗黙の信頼ゾーン」と呼びます。フラットなオフィスネットワークも、同じように動きます。ゼロトラストは、判断とその適用をリソースの近くへ移し、信頼ゾーンをできるだけ小さく保ちます。

概念を判断に生かす

「ゼロトラストとは？」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。 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

従来のモデルは、組織の周りに1本の境界を引き、内側を信頼します。NISTの異論は明快です。攻撃者が境界を破ると、内部を横方向に移動するのを妨げるものがなくなります。文書が対象とする政府機関にとって、許可のない横移動は、最大級の課題の1つでした。境界も、仕事の実態に合わなくなっています。職員は自宅やホテルのネットワークからサインインし、一部のシステムは個人の端末を認め、利用するものの多くは他者のクラウドで動きます。ここからNISTの前提が導かれます。プライベートネットワークは暗黙の信頼ゾーンではなく、攻撃者はすでに内部にいるかもしれず、遠隔勤務の職員は、接続元のローカルネットワークを敵対的なものとして扱うべきです。

得られるのは、被害範囲の限定です。NISTの7原則の3番目では、アクセスはセッションごとに、作業に必要な最小の権限で許可します。1つのリソースで認証しても、別のリソースに権限は生まれません。盗まれたパスワードや侵害されたノートパソコンが到達できるのは、内部ネットワーク全体ではなく、その時点で、そのアカウントと端末に、1つの適用点を通して許された範囲です。判断は証跡も残します。ポリシーエンジンは、許可と拒否をすべて記録するため、誰が、なぜシステムに到達できたかを、記憶ではなく記録から答えられます。

実際の活用例

購買システムを考えます。組織全体が依存するメールとは違い、決まった職員の集団が使うため、NISTが最初の移行候補として挙げる種類のアプリケーションです。購買担当者が会社のノートパソコンから開くと、要求はアプリケーションの手前の適用点に届き、そこからポリシーエンジンに問い合わせます。エンジンの信頼評価アルゴリズムは、NISTが挙げる入力を検討します。端末のOSバージョンとパッチの水準を含む要求自体、主体のデータベース、資産のデータベース、認証保証レベルを指定したり国外のアドレスを拒否したりするリソース固有の要件、そして脅威情報です。以下は、製品のものではなく、当社で考えた項目名を使う、判断記録の説明用の例です。

```
要求       buyer-17、端末laptop-0417 -> 購買アプリ、読み取りと書き込み
主体       調達チーム。フィッシング耐性のある鍵でサインイン
資産       企業が管理し、OSパッチは最新、ディスクは暗号化済み
リソース   AAL2以上、管理対象の端末、国内の送信元IPが必要
脅威       送信元アドレスは、参照した脅威情報フィードに記載なし
判断       このセッションに限り読み書きを許可し、承認として記録
```

許可が対象とするのは、この1セッションと、この1アプリケーションだけです。同じ担当者が、同じノートパソコンで、文書ストアにある仕入先の契約書を開くと、エンジンは新たにアクセスを判断します。最初のリソースの認証が、2つ目のアクセスを自動的に許可することはありません。状況も重要です。NISTの例には、通常は営業時間内に働く経理担当者が、突然、深夜に、エンジンが認識していない場所から財務システムを要求するものがあります。状況に応じた信頼評価アルゴリズムなら、警告を出し、まず主体に、より厳しい信頼水準を満たすよう求められます。別の例は、通常1日に20件から30件の人事記録を読む人事担当者が、100件を超えて要求する場合です。

クラウドサービスについてNISTは、まずVPNで内部ネットワークへ入れなくても、クライアントがサービスに直接アクセスでき、その経路上で組織の適用点がポリシーを検査できると指摘しています。こうした判断はすべて、誰が何にアクセスすべきかを明確に把握していることが前提です。そのためNISTは、何かを構築する前に、資産、主体、データの流れ、業務の流れを調査するよう求めています。この土台づくりは、当社のM365とSSOを横断するアクセス管理の事例で説明する統合と同種のものです。M365、1Password、Red Hat SSO、OKTA SSOのIDとアクセスをまとめ、最小権限を徹底し、入社・退社時の手順を標準化することで、アクセスの付与と取り消しを速やかに行いました。

問題が起きるところ

製品として買う。 NISTは、ゼロトラストを単一のアーキテクチャではなく指針の集合とし、ゼロトラスト企業向けのツールやサービスも、1つの組み合わせに決まるものではないと述べています。箱に名前の付いた新しい遠隔アクセス用ゲートウェイでも、通した全主体が背後のネットワーク全体に到達できるなら、大して変わりません。対策は、NISTの言う「一括置換ではなく、段階を踏む取り組み」として、業務の流れを1つずつ移すことです。各製品を、満たすべき原則に照らして判断し、後で別の提供者に移れるデータ形式かどうかも検討します。

台帳を作る前にポリシーを書く。 ポリシーエンジンは、主体、資産、手順について知っている情報だけで判断できます。NISTは、情報が不完全な場合、通常は情報不足を理由にエンジンが要求を拒否し、業務が止まると警告しています。IT

部門の管理外に構築されたシステムであるシャドーITは、問題を悪化させます。対策は、まずシャドーITを含む資産、主体、データの流れ、業務の流れを調べて台帳にまとめ、その後で、移行候補の業務の基準を書くことです。

管理者だけ包括的なアクセスを保つ。 古い設計の多くは、開発者やシステム管理者が全リソースに到達できます。NISTは、これらのアカウントを、特に厳しく調べる対象としています。ほかの全員にはセッションごとの判断を課しながら、管理者アカウントには常時アクセスを残すと、最も価値のある認証情報が、侵入の最短経路のままです。対策は、特権アカウントも同じエンジンを通し、現在の作業に必要なアクセスを与え、ログと監査で通常の使い方を把握し、逸脱を目立たせることです。

ポリシーエンジンが新しい境界になる。 エンジンと管理機能が承認しなければ、リソース同士は通信できません。エンジンの規則にアクセスできる人は、無承認の変更や単純な間違いを加えられます。適用点や管理機能を妨害する攻撃者は、業務を止められます。対策は、設定変更をすべて記録して監査し、適切に保護されたクラウド環境でポリシーを適用するか、複数の拠点に複製することです。保存した通信データとポリシーには、専用の管理者アカウントだけがアクセスできる、最も厳しい制限をかけます。

初日から全面的に強制する。 初回から正しいポリシーは少なく、NISTも、本来通るべき要求が拒否される調整期間を想定しています。直ちに厳格な強制へ切り替えると、ポリシーの不足がすべて、職員が必要な仕事から締め出される事態になります。対策は、新しい業務の流れを、しばらく報告だけのモードで動かすことです。要求の大半を許可し、ログを意図したポリシーと照合し、MFAに失敗した要求や、敵対的と分かっているIPアドレスからの要求を拒否するなど、基本だけを強制します。通常の状態を理解してから、ポリシーを厳しくします。

MFAで完成とする。 MFAは、盗まれたパスワードが悪用されるリスクを下げます。ただしNISTは、有効な認証情報を持つ攻撃者や、悪意のある内部者が、そのアカウントに許されたものには、引き続き到達できると指摘しています。対策は、各アカウントの到達範囲を狭く保ち、時刻、場所、量を検討する、状況に応じた信頼評価アルゴリズムを使うことです。正しい認証情報でも、通常と異なる使い方には警告を出せます。

参考資料

- NIST SP 800-207: ゼロトラストアーキテクチャ — 2020年8月公開。定義、7原則、論理的な構成要素、脅威、移行の道筋。

- NIST SP 1800-35: ゼロトラストアーキテクチャの実装 — 2025年6月公開のNIST実践ガイド。24の協力組織と構築した、19の実装例を説明します。
- NIST SP 800-207A — 2023年9月公開。ネットワークアドレスではなく、APIゲートウェイ、サイドカープロキシ、サービスのIDに基づく、複数クラウドにまたがるクラウドネイティブアプリケーションのアクセス制御。
- NIST SP 800-63B-4 — リソースの要件で指定できる認証保証レベル。AAL3はフィッシング耐性を求めます。

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

「ゼロトラストとは？」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/zero-trust/