Engineer

ホスト

ネットワークに接続したコンピューター

どのようなものか

ホストは、ネットワーク経路の端にあるコンピューターです。通信を中継するだけのルーターやスイッチに対し、通信の宛先になり、送信元にもなるマシンを指します。技術者は「ホストマシン」とも呼び、応答に使う名前を「ホスト名」といいます。仮想化では、ゲストマシンを動かす物理ホストを指します。ウェブホスティングのように、何かを「ホストする」とは、そのようなマシン上で動かすことです。

インターネット自体による定義は、1989年10月にさかのぼります。インターネットホストの要件を定めるRFC 1122は、ホストコンピューター、略してホストを、通信サービスの最終的な利用者で、通常は利用者のためにアプリケーションプログラムを実行するマシンと説明します。OSIモデルでいうエンドシステムに当たります。ホスト間のネットワークは、現在ルーターと呼ばれるゲートウェイで接続されます。同じ文書は、単一目的のホストから多機能なホストまでを扱い、複数のネットワークインターフェースを持つホストをマルチホームと呼びます。

ホストとルーターの境界を決めるのは、ハードウェアではなく動作です。RFC 1122は、「別のホストが生成したデータグラムを転送する」ホストは「ゲートウェイとして動作している」とし、その機能を無効にする設定を求め、初期状態では無効でなければならないとします。ネットワークインターフェースが二つあっても、それだけでホストが転送を始めるわけではありません。ノートパソコン、電話、プリンター、借りた仮想マシン、独自のアドレスを持つコンテナーは、いずれもホストです。

NISTの用語集は、二つの定義を並べています。一つは、ネットワークへ接続する手段のあるハードウェア機器すべてを含めます。もう一つは、ウェブサーバーの保護に関する指針からの定義で、クライアントから見ればサーバーもホストであり、クライアント端末も、通信を振り分けるルーターやスイッチと違い、「ネッ

トワークに対する情報源」であるためホストとします。サーバーという言葉との違いは、ここにあります。サーバーは、要求へ応答するプログラムの役割です。ホストは、誰かに応答するかどうかを問わず、そのマシンです。一台のホストで多数のサーバーを動かせますし、一つも動かさないノートパソコンもホストです。

ホストには、いくつもの名前が付きます。関連文書のRFC 1123は、ホスト名の規則を定めました。先頭文字には英字だけでなく数字も使え、ホストのソフトウェアは63文字までの名前を扱えなければならず、255文字まで扱えることが推奨されます。また、利用者がホスト名を入力できる場所では、ドット区切りの十進表記でアドレスを入力しても動くことが推奨されます。さらに、DNSでは任意の数の名前を一つのアドレスへ向けられ、HTTPでは、各要求の `Host` フィールドで、どの名前を求めるかをクライアントが伝えられます。そのため、一台のホストで多数のサイトに応答できます。

概念を判断に生かす

「ホストとは？」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。 実際の使用量に合わせてサーバーを構成し、月額費用を事前に把握したうえで、クラウドへの移行もクラウドからの移転も進めます。

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。 Google Cloud・AWSでDockerアプリ20個を運用 — 20 デプロイし監視したコンテナアプリケーション

Google Cloud・AWSでDockerアプリ20個を運用 お問い合わせ →

なぜ重要なのか

ホストは、運用で数える単位です。構成管理台帳にホストが並び、監視がホストを見守り、ファイアウォールの規則やアクセスリストがホストを指定し、クラウド事業者が時間単位や月単位でホストに課金します。「容量を増やす」と違い、「ホストを追加する」という計画は具体的です。作成し、名前を付け、パッチを当て、バックアップし、料金を支払うマシンが、もう一台増えることを意味します。

侵害の単位でもあります。ホストを支配した者は、その上のすべてのサーバープログラム、ディスクに保存したすべての鍵、そこから確立できるすべての接続を支配します。何を置くかで、失ったときの損害が決まります。そのため、慎重な運用者は、秘密情報、データ、ネットワーク経路をホストごとに決め、必要なものだけを与えます。

名前が集まる場所でもあります。同じマシンが、台帳上の名前、自分自身に付けた名前、アドレスへ向くDNS名、受け取る要求内の名前で知られています。それらが一致すれば、ログ一行、警報、問い合わせチケットが、同じマシンを指します。食い違うと、夜中に呼び出された担当者は、インシデントの最初の数分を、対象のマシン探しに費やします。

実際の活用例

このサイトの運用では、ホストをコードから構築し、専用の秘密情報を与える対象として扱います。別の事業者に二台目が必要になったとき、リポジトリーから二台目のホストを作成し、既存なら再び管理下へ取り込みます。一台目は手作業で作り、後からファイアウォールを設定していたため、初期パスワードポリシーのまま、新しいホストへインターネットから到達できる時間が生じます。二台目を作るロールは、既存マシンがあれば重複作成せず管理下へ取り込むので、再実行しても安全です。リポジトリー内で、実行すると費用が発生する唯一のロールであるため、専用ファイルにインスタンスの種類、リージョン、仕様、ユーロ建ての月額を記載します。

一台から二台に増やすと、今後も一台しかないと想定して書いた値が、すべて表面化しました。運用上の秘密情報を、それぞれホストをキーにしたマップへ変えました。事例は、共有が不適切な理由を二つ記録します。二台で共有するデッドマンスイッチは、別々のスイッチ二つより警報は増えず、かえって減ります。一方が動作報告を続ければ、もう一方が停止しても正常のままになるためです。また、バックアップのパスフレーズを共有すると、ホストごとの情報漏えいリスクが結び付きます。同じパスフレーズを使っていても、別々のresticリポジトリーは異なるマスターキーを持つ場合があります。ただし、そのパスフレーズを入手し、両リポジトリーの暗号化データと鍵ファイルを読める相手は、両方を復号できます。既存ホストは四つすべてのマップに登録し、リポジトリーと二つのスイッチは空のままにしました。事例は、それを実態に忠実な状態と呼びます。

閲覧者にとっては、もっと小さな意味になります。ブラウザーが接続する名前です。セキュリティのページは、ブラウザーのネットワークパネルを開いてホストを数えるよう案内し、一つだけで、それはサイト自身のホストだと説明します。

問題が起きるところ

受信するだけのはずのホストが、通信を転送し始めます。 コンテナーネットワークやVPNソフトウェアがIP転送を有効にすると、ホストはインターフェース間を経路制御します。たとえばDockerの文書は、起動時に以下の二つの設定を有効にし、その後、許可する規則がなければ転送パケットを破棄すると説明しま

す。そのような規則がないまま転送が有効になっている場所では、ホスト自身宛ての通信に対するファイアウォール規則は、通過する通信を扱いません。その背後のネットワークへ、誰も図に描いていない経路から到達できるようになります。設定を確認し、`1`になっている場所では、意図して転送規則を書きます。

```
sysctl net.ipv4.ip_forward net.ipv6.conf.all.forwarding
```

名前が一致しません。 台帳にはある名前があり、マシン自身は事業者のイメージが選んだ名前を名乗り、DNSには三つ目、TLS証明書には四つ目の名前があります。すると、どの警報にも、誰も使わない名前が付きます。マシン自身のホスト名を、台帳やDNSレコードと同じ情報源から取り、誰かが気付いたときではなく、ホストの作成時に設定します。

渡されたどのホスト名にも、サーバーが応答します。 `Host`フィールドはクライアントから届きます。未知の名前にも既定サイトで応答するサーバーは、攻撃者が選んだ名前から、リンク、転送先、キャッシュするページを組み立ててしまいます。RFC 9110は、このフィールドが「共有キャッシュを汚染する、または意図しないサーバーへ要求を転送する」マルウェアの、頻繁な標的だと警告します。実際に提供する名前だけに応答し、ほかは拒否し、絶対リンクは要求からではなく設定から組み立てます。

複製したホストが、同じ識別情報を共有します。 イメージからコピーしたマシンには、SSHホスト鍵、トークン、ときにはバックアップのパスフレーズなど、イメージにあったものが残ります。クライアントはコピーを見分けられなくなり、一件の漏洩で全コピーへ侵入できるようになります。初回起動時にホスト鍵を生成し、秘密情報はイメージへ入れず、秘密情報を設定するすべての場所で、ホストごとに専用の項目を与えます。

参考資料

- ホスト — NIST CSRC用語集 — ホストをルーターやスイッチと区別する定義を含む、二つの定義です。
- RFC 1122：インターネットホストの要件、通信層 — 1989年のホストの定義、マルチホーム、初期状態で無効な転送の説明です。
- RFC 1123：インターネットホストの要件、アプリケーションと支援機能 — 第2.1節の、ホスト名とその長さの規則です。
- RFC 9110、HTTPの意味：Hostと:authority — 一つのサーバーが多数のホスト名を区別する方法と、このフィールドが標的になる理由です。

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

「ホストとは？」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/host/