Engineer

ポート

ホスト内のサービスを選ぶための番号

どのようなものか

ポートは、各TCPセグメントとUDPセグメントのヘッダーにある16ビットの数値で、受信側のマシンに、どのプログラム宛てのデータかを伝えます。アドレスがパケットを適切なホストへ届け、到着後はポートが適切なプロセスへ届けます。厳密に言うときは、ポート番号と呼びます。複数のポートと言えば、通常はサーバーが待ち受ける番号の集合です。スイッチの物理的な接続口や、別のプラットフォームへソフトウェアを移植するという意味のportとは、関係ありません。

フィールドの幅が16ビットなので、65,536通りの値があり、範囲は0から65535です。TCPとUDPは別々の番号の集合を持ち、TCPのポート53とUDPのポート53は別物ですが、DNSは両方を使います。TCPの仕様RFC 9293は、インターネットアドレスとポートを組み合わせたものをソケット、二つのソケットの組を接続と定義します。値は、クライアントのアドレス、クライアントのポート、サーバーのアドレス、サーバーのポートの四つです。一つのサーバーポートで何千もの通信を同時に扱える理由も、ここにあります。それぞれの通信で、残りの三つの値の少なくとも一つ、通常はクライアントのポートが違います。

RFC 6335は、番号の範囲を三つに分けます。0–1023はシステムポート、1024–49151はユーザーポート、49152–65535は動的ポートで、IANAは動的ポートを割り当てません。IANAはサービス名と番号の対応を登録する台帳を管理します。SSHは22、DNSは53、HTTPSは443、PostgreSQLは5432です。登録は、クライアントが頼る慣例です。どのプログラムも空いている番号で待ち受けられるため、SSHを推測しにくいポートへ置くこともできます。

通常、接続のクライアント側には、自分で選んでいないポートが割り当てられます。プログラムが外へ接続するときは、OSが一時ポートの範囲から選びます。Linuxの既定値はIANAの動的範囲ではなく、32768–60999です。ポート0へのバインド要求も、「空いている番号を一つ割り当てる」という意味になります。

概念を判断に生かす

「ポートとは？」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。 Wi-Fi、ファイアウォール、リモートアクセスを整え、どこからでも働け、権限のある人だけが接続できるようにします。

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。 Ubuntu Linux VPSインスタンス30台を管理 — 30 復旧計画とともに管理したLinuxサーバー

Ubuntu Linux VPSインスタンス30台を管理 お問い合わせ →

なぜ重要なのか

ポートを決めるときに問うのは、何を公開するかです。外部からの要求に応答するプログラムと、その待ち受けアドレスを決めます。待ち受けのないポートへの接続は拒否されます。待ち受けがあるポートには、そのアドレスへ届く誰もが、欠陥も含めたソフトウェアとやり取りできます。保護にかかるコストが最も低いのは、127.0.0.1で待ち受けるサービスです。ファイアウォールの設定にかかわらず、別のマシンからのパケットは、ループバックアドレスへ到達できません。

そこで、各サービスに最初に問うのは、そもそも外部から届く必要があるかです。同じマシン上のアプリケーションだけが使うデータベースは、ループバックに置きます。管理者だけが使うツールも、ループバックで待ち受け、踏み台ホストやVPN経由で利用できます。残ったもの、通常はウェブサイト用の80と443、SSH用の一つのポートが、公開面になります。公開して待ち受ける各サービスには、パッチ、ログ、それに合ったファイアウォール規則が必要なので、公開面を小さくするのは、セキュリティー面と同じくらい、コスト面での判断でもあります。

二つ目は番号です。標準ポートなら、余分な設定は要りません。ブラウザー、クライアント、制限の厳しいネットワークは443を想定し、通します。SSHを22以外へ移すと、既定の番号だけを試すスキャナーの雑音が減り、ログを読みやすくなります。ただし、全範囲を走査すれば見つかり、ポートを参照するすべてのツールへ、新しい番号を伝える必要があります。忘れやすいのは、この最後の部分です。

三つ目は、権限と共有です。Linuxでは、1024未満のポートへバインドするにはrootかCAP_NET_BIND_SERVICEケーパビリティーが必要です。ただし、ip_unprivileged_port_startを既定の1024から下げた場合は例外です。通常、特定のアドレスとポートは、一つのプログラムが占有します。そのため、二つのサービスが443を使うなら、手前で通信を振り分けるものが必要です。一般には、クライアントが求めたホスト名を読むリバースプロキシを使います。

実際の活用例

自社でGitフォージを設けた2026年7月には、フォージのSSH待ち受けを、ループバックのポート23231へバインドしました。外からは踏み台ホストを通るので、公開ポートの数は変わりませんでした。各接続の冒頭のバイト列を見て、一つの公開ポートからHTTPSとSSH経由のGitを提供するマルチプレクサーは、実装済みですが無効にしています。利用者のいない待ち受けでも、防御する必要があるためです。

2026年8月の強化レビューでは、ホストの最初の強化時にSSHをポート1986へ移した一方、侵入者を遮断するjailは22を監視し続けていたことが分かりました。jailによる遮断は、毎回、待ち受けのないポートを塞いでいました。そのため、この保護は一度も機能していませんでした。修正は小さなものでしたが、「各セキュリティー制御に、それを実際に動かして確かめるアサーションを組み合わせる」という規則が残りました。

ホストのメモリーは464 MBで、ダッシュボードはありません。そこで、稼働中のマシンをMarkdownで示す、七つの読み取り専用レポートロールで状態を調べます。基本情報のレポートは、待ち受けソケットを列挙します。設定に書いたポート一覧ではなく、カーネルが実際に持つ一覧です。レポートが実際に発見したものの一つは、どの定義にも書かれていない待ち受けポートでした。

問題が起きるところ

マシン内だけで使うはずのサービスが、インターネット全体へ応答します。 多くのプログラムは、既定ですべてのアドレスで待ち受け、ソケット一覧では `0.0.0.0` 、 `[::]` 、 `*` と表示されます。その状態では、ローカル専用のデータベースや管理画面も、ファイアウォールを一度設定し損なうだけで公開されます。バインド先を `127.0.0.1` か `::1` へ明示的に設定し、ローカルアドレス欄で確かめます。

```
ss -tlnp
ss -ulnp
```

サービスを移した後も、保護機構が古いポートを見ています。 サービスの番号は変わったのに、ファイアウォール規則、遮断用jail、監視プローブ、クライアント設定のいずれかが、元の番号を指しています。各ツールは、デーモンがいな

いポートを相手に、正しく動き続けます。番号を、利用するすべての仕組みが読む一つの変数へ置き、待ち受けソケットと各制御の監視対象を比較する検査を追加します。

負荷が増えると、外向きの接続が「Cannot assign requested address」で失敗し始めます。 各外向き接続は一時ポート範囲のローカルポートを一つ使い、閉じた後もしばらくは、四つの値をTIME_WAITで予約したままにします。Linuxの既定の32768–60999なら、一つのクライアントアドレスが、同じサーバーアドレスとポートに対して保持できるのは、接続中または閉じた直後の28,232接続です。同じバックエンドへの要求ごとに接続を作るプロキシやワーカーは、この範囲を使い切ります。まずkeep-aliveやプールで接続を再利用します。範囲を広げたり、送信元アドレスを増やしたりしても、余裕を増やすだけです。

一般ユーザーとして起動したサービスが、ポート80で「Permission denied」となって止まります。 1024未満へのバインドには権限が必要です。ユニットファイルでCAP_NET_BIND_SERVICEケーパビリティーを与えるか、高い番号のポートに置いて手前にリバースプロキシを設けます。ローカルユーザーを全員信頼するホストなら、ip_unprivileged_port_startを下げる方法もあります。一つのポートのためにサービス全体をrootで動かすのは、最も悪い選択です。

起動が「Address already in use」で止まります。 別のプロセスがポートを使っています。終了処理中の同じサービスの旧プロセスや、同じ既定値を使う別のサービスであることがよくあります。8080は、よく使われる番号です。`ss -tlnp` で所有者を調べます。番号をどのサービスが使うか決め、既定値に頼らず、それぞれの設定にポートを明記します。

参考資料

- RFC 9293、第4節：用語集 — TCPの仕様自身による、ポート、ソケット、接続の定義です。
- RFC 6335：サービス名とトランスポートプロトコルのポート番号の登録を管理するIANAの手順 — 三つのポート範囲と、番号の割り当て方です。
- サービス名とトランスポートプロトコルのポート番号の登録簿 — どの番号に、どのサービスが登録されているかを示すIANAの一覧です。
- RFC 768：User Datagram Protocol — 送信元と宛先のポートを含む、三ページのUDP仕様です。
- RFC 6056：トランスポートプロトコルのポートをランダム化するための勧告 — クライアントが一時ポートを推測されにくく選ぶ方法です。
- IP Sysctl — ip_local_port_rangeとip_unprivileged_port_startを含む、Linuxカーネルの設定です。

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

「ポートとは？」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/port/