Engineer

IPアドレス

パケットの配送先をネットワークに伝える数値

どのようなものか

IPアドレスは、Internet Protocolが各パケットに書き込み、その行き先を示す数値です。その隣には、送信元を示す別のアドレスがあります。IPバージョン4の1981年の仕様RFC 791は、これをインターネットアドレスと呼び、「アドレスは、その所在を示す」と一文で役割を説明しています。ドメインなどの名前は、探しているものを示すため、まずアドレスに変換する必要があります。それがDNSの仕事です。二つのアドレスを結ぶ経路は、その間のルーターが決めます。

IPv4のアドレスは32ビット、四つのオクテットからなり、0から255までの十進数四つをドットで区切って、192.0.2.10のように書きます。RFC 791は、そのビットをネットワーク番号とローカル部分に分け、三つの固定クラスで区切りの位置を決めました。このクラス分けは、大半の組織には合いませんでした。クラスCのネットワークは最大254ホスト、クラスBは最大65,534ホストを収容できたため、経路表が大きくなる一方で、クラスBの番号が不足しました。1993年9月のRFC 1519は、クラスをCIDRに置き換えました。任意のビットの後で区切ることができ、その位置をスラッシュの後に書きます。192.0.2.0/24は、最初の24ビットを固定した、256アドレスのブロックです。

IPv6は、アドレスを128ビットに広げます。最大四桁の十六進数を八組、コロンで区切って書きます。RFC 4291は、連続するゼロの組を一か所だけ `::` に縮めることを認めるため、2001:db8:0:0:0:0:2:1は、2001:db8::2:1とも書けます。同じアドレスを多くの形で書けるため、後のRFC 5952が、推奨する一つの表記を定めました。小文字を使い、各組の先頭のゼロを除き、最も長くゼロの組が続く箇所に `::` を使います。

アドレスは、マシンではなく、ネットワークインターフェースに属します。RFC 791も、単一のホストが複数のインターネットアドレスで複数のホストとして振る舞える必要があり、物理インターフェースをいくつも持つホストもあると述べていました。RFC 4291は、ほかにどんなアドレスがあっても、各IPv6インターフ

ェースに、自身のネットワーク区間内だけで有効なリンクローカルアドレスを少なくとも一つ持たせるよう求めています。そのため、両方のバージョンを動かすネットワークのホストは、自分自身に接続するループバックアドレスに加え、複数のアドレスを同時に持ちます。ループバックには、IPv4の127.0.0.0/8ブロックと、IPv6の `::1` を使います。

どのアドレスにも、どこからでも接続できるわけではありません。RFC 1918は、10.0.0.0/8、172.16.0.0/12、192.168.0.0/16という三つのIPv4ブロックをプライベートネットワーク用に確保し、その経路情報を組織間で伝えてはならないとしています。そのため、これらのアドレスを持つ機器は、NATなど、代わりとなる仕組みを通してのみインターネットに接続します。RFC 3022は、NATを、外へ出る際にプライベートアドレスをパブリックアドレスに変換する仕組みと説明しています。さらに、RFC 5737は、192.0.2.0/24、198.51.100.0/24、203.0.113.0/24という三つのブロックを文書用に予約し、RFC 3849は、IPv6の2001:db8::/32について同じことをしています。この記事で例に使うアドレスはすべて、これらの文書用範囲から取っています。

概念を判断に生かす

「IPアドレスとは？」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

アドレスは、サーバーがクライアントについて必ず持つ情報です。なければ、応答の宛先がありません。そのため、多くの判断で既定のキーになります。ファイアウォールの規則はアドレスで許可と遮断を決め、レート制限はアドレスごとの要求数を数え、アクセスログは毎行記録し、不正利用の報告もそれを示します。どれも、アドレスが、意図した対象を正しく識別できる範囲でのみ機能します。

アドレスで識別できることは、想像ほど多くありません。NATの内側では、オフィスや家庭の全機器が、同じパブリックIPv4アドレスからインターネットに接続できます。その一台に向けた遮断や制限は、全機器に及びます。プロキシーやCDNの背後では、サーバーがどの要求でも見るのはプロキシーのアドレスです。

クライアント自身のアドレスが届くとしても、誰か別の主体が書いたヘッダーで届きます。アドレスを基準にした規則は、ネットワーク上の位置に関するものであり、人に関するものではありません。

同時に、予想より多くの情報を明かします。プロキシーがクライアントのアドレスを伝える `Forwarded` ヘッダーを標準化したRFC 7239は、プライバシーの節で、IPアドレスからクライアントを一意に識別できたり、利用する事業者が分かったり、おおよその場所を推測できたりすると指摘しています。アドレスで埋まるログは、役に立つ一方で危険も伴います。だからこそ、記録を始める前に、何を残すかを決めることが大切です。

現在は、二種類のアドレスがあります。アドレスを解析、保存、比較するものは、IPv4とIPv6の両方に対応する必要があります。両方を提供するネットワークのクライアントは、どちらから来る可能性もあるためです。すべてのアドレスが数字とドットの十五文字に収まった時代のコードは、最初のIPv6訪問者で壊れます。多くの場合、アドレスを読み込んだ場所から遠く離れた箇所で起きます。

実際の活用例

Pythonの標準ライブラリーには、両バージョンを解析し、計算も行う `ipaddress` モジュールがあります。文字列を手で分割する必要はありません。対話セッションでは、次のように使います。

```
>>> import ipaddress
>>> ipaddress.ip_address("203.0.113.57")
IPv4Address('203.0.113.57')
>>> ipaddress.ip_address("2001:0DB8:0000:0000:0000:0000:0002:0001")
IPv6Address('2001:db8::2:1')
>>> ipaddress.ip_network("203.0.113.57/24", strict=False)
IPv4Network('203.0.113.0/24')
>>> ipaddress.ip_network("2001:db8:42:7::5/48", strict=False)
IPv6Network('2001:db8:42::/48')
```

二つ目の呼び出しは、RFC 5952が求める正規化を示します。大文字の長い表記と小文字の短い表記は同じアドレスであり、モジュールは正規形を出力します。192.0.2.300のような文字列は、300が一オクテットに収まらないため、`ValueError` で拒否します。最後の二つの呼び出しは、アドレスから、それを含むネットワークを求めます。 `strict=False` がなければ、203.0.113.57/24にはホスト部のビットが立っているため、こちらも拒否します。指定するとホスト部をゼロにし、ネットワークだけを残します。

このサイトのウェブアクセスログは、訪問者のアドレスに同じゼロ化を行います。プライバシーのページによると、ウェブログの行を書く時点で、ディスクに届く前にアドレスの末尾をゼロに置き換えます。保存値が示すのは大まかなネットワークで、その範囲ではオフィス全体や通り全体が同じに見えることがあります。サーバーは二つの名前でアドレスを記録するため、両方をマスクし、独自のアドレスを含み得るヘッダーを行の書き込み前に除去します。何ビット残すかは述べていません。上の/24と/48は、この記事の説明用で、サイトの設定ではありません。記録時にマスクすれば、後処理のジョブに頼らず、完全なアドレスをそのウェブログに残さずに済みます。同じプライバシーページは、Gopherについて別の扱いも記しています。OSが接続ごとに記録するログには送信元アドレスが含まれ、三十日後に保存期限を迎えます。

問題が起きるところ

ヘッダーの値をクライアントのアドレスとして信頼します。 `X-Forwarded-For` と標準の `Forwarded` は、通常の要求ヘッダーです。RFC 7239は、クライアントとサーバーの間のどの中継点も、クライアント自身も、誤って、あるいは意図的に `Forwarded` を書き換え得ると警告しています。一覧の最初のアドレスを使うコードは、クライアントが自分のアドレスを選び、それに伴って自分のレート制限や許可リスト上の扱いも選べるようにしてしまいます。自分が運用するプロキシーを通った要求でなければ、TCP接続のアドレスを使います。通った場合も、右から数えて、自分のプロキシーが追加した部分だけを読みます。

アドレスを人と見なします。 多くの利用者が同じアドレスを共有するため、アドレス単位の遮断でオフィス全体を締め出したり、一人向けの制限で学校全体の通信を制限したりしかねません。アドレスは粗い単位の判断に使い、共有を考慮して制限を設定し、個人に関するものは、代わりに認証済みアカウントに結び付けます。

アドレスを文字列として比較します。 2001:db8::2:1と2001:DB8:0:0:0:0:2:1は、一つのアドレスを表す異なる二つの文字列です。文字列照合の許可リストでは、一方を受け入れて他方を拒否します。比較前に両方を解析するか、RFC 5952の表記だけを保存します。

IPv4だけを解析します。 ドット区切りの四つの数値に対応する正規表現、十五文字分の列、最後のコロンでホストとポートを分けるコードは、どれもIPv6で失敗します。適切なパーサーを使い、両バージョンに対応する列型や長さを選びます。IPv6アドレスにポートを併記する場合、RFC 5952は、[2001:db8::1]:443のような角括弧を勧めています。なければ、最後の組をアドレスの一部と読めてしまうためです。

必要以上に長く、完全なアドレスを残します。 止める仕組みがなければ、ログ、分析表、バックアップに、何年もアドレスがたまります。必要な精度を決め、後からではなく書き込む時点で短縮し、残した部分にも保存期限を設けます。

実在するアドレスを例に使います。 設定例、テスト用データ、スクリーンショットに誰かの実アドレスを使うと、コピーした設定から、無関係な相手に通信が届きます。RFC 5737は、まさにそのような衝突や混乱を減らすため、三つのブロックを予約しています。それらと、IPv6用の2001:db8::/32を使います。

参考資料

- RFC 791：Internet Protocol — IPv4の1981年の仕様です。32ビットのアドレスと、名前、アドレス、経路の違いを扱います。
- RFC 4291：IPバージョン6のアドレス体系 — IPv6のアドレス種別、テキスト表記、リンクローカルアドレスの要件です。
- RFC 5952：IPv6アドレスのテキスト表記に関する推奨事項 — IPv6アドレスの正規表記と、自由なつづり方から生じる問題です。
- RFC 7239：Forwarded HTTP拡張 — プロキシーがクライアントのアドレスを伝える方法、結果をそのまま信頼できない理由、プライバシー上の代償です。
- RFC 5737：文書用に予約したIPv4アドレスブロック — 例に使う三つの範囲です。
- ipaddress：IPv4/IPv6操作ライブラリー — アドレスの解析、比較、グループ化に使う、Pythonの標準モジュールです。

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

「IPアドレスとは？」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/ip-address/