Engineer

DHCP

IPアドレスと設定を機器へ貸し出すプロトコル

どのようなものか

DHCP、Dynamic Host Configuration Protocolは、新しくネットワークへ接続した機器が、そのネットワーク内で使う設定を知る仕組みです。Wi-Fiへ接続したノートPCは、自分のハードウェアアドレス以外、ほとんど何も知りません。DHCPは、誰も入力しなくても、IPアドレス、サブネットマスク、トラフィックを送るルーター、問い合わせ先のDNSサーバーを渡します。1997年3月に公開されたRFC 2131が、プロトコルを定義しています。要旨では、TCP/IPネットワークのホストへ、構成情報を渡す方法としています。以前のBootstrap Protocol、BOOTPから発展しました。主な追加点は、再利用できるアドレスを自動で割り当てる仕組みです。

RFC 2131は、アドレスを渡す三つの方法を挙げます。自動割り当てでは、クライアントに恒久的なアドレスを与えます。動的割り当てでは、一定期間、またはクライアントが返却するまでのアドレスを与えます。手動割り当てでは、管理者がアドレスを選び、DHCPは届けるだけです。割り当て先がそのアドレスを必要としなくなった後、自動でプールへアドレスを戻せるのは、この三つのうち、動的割り当てだけです。以下では、この方式を扱います。

アドレスを貸す期間を、リースと呼びます。クライアントは、延長も、早期返却もでき、無期限のリースを要求することもできます。RFCは、それでもサーバーが、長いが有限のリースを選ぶ場合があると記します。クライアントが使われなくなったことを、いずれ検知できるようにするためです。サーバーの背後には、RFCが永続ストレージと呼ぶものがあります。識別子をキーに、クライアントごとに一件の記録を持ち、渡したパラメーターを保持します。

DHCPはUDPで動きます。クライアントはサーバーのポート67へ送り、サーバーはクライアントのポート68へ答えます。サブネットマスクからリース時間まで、渡せるオプションは、別のRFC 2132が規定します。IPv6にはDHCPv6という独自のプロトコルがあり、現在は、2026年1月のインターネット標準、RFC 9915が規

定しています。RFC 8415を置き換えたものです。ポートも別で、クライアントは546、サーバーとリレーエージェントは547を使います。ステートレスアドレス自動設定、SLAACの代わりにも、併用にもできます。RFC 9915自身は、区別が必要なとき、IPv4のプロトコルをDHCPv4と呼びます。また、IPv4の設定情報は、DHCPv6ではなくDHCPv4で運ぶことを推奨する、IETFの合意を記しています。

概念を判断に生かす

「DHCP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

ネットワークのどの機器にも、同じ少数の設定が必要で、一つ間違うだけでも接続できなくなります。サブネットと合わないマスク、別の相手のものであるルーターアドレス、去年止めたDNSサーバーなどです。DHCPがなければ、すべての値を各機器へ入力し、変更のたびに正しく保たなければなりません。DHCPなら、一か所で保持します。オフィス全体のDNSサーバー変更は、建物を歩き回る作業ではなく、サーバー設定の変更になります。

規模を大きくできる理由は、リースです。動的割り当ては、期間を決めて貸すため、すべての機器が同時に接続するのでない限り、一週間で、アドレス数を超える台数へ提供できます。RFC 2131は、一時的にしか接続しないクライアントや、恒久的なアドレスを必要としないクライアント間で、限られたプールを共有するときに、特に有用だとします。クライアントは、何も言わずに消える場合もあります。そのため、プロトコルは別れの挨拶に頼りません。正常な動作は、クライアントが解放メッセージを送るかどうかに依存しないと、RFCは明記しています。持ち主が通知しなくても、期間が切れればアドレスは戻ります。

そのため、リース期間は、既定値のまま放置するものではなく、実際の設計判断です。長いリースでは、ネットワークから離れた機器のアドレスを、ほかの機器が使えない状態で長く保持します。短いリースでは、更新の通信が増えます。また、応答をやめたサーバーを直す時間も短くなります。サーバーへ到達する前に期間が切れたクライアントは、そのアドレスを使うのをやめなければならないためです。

DHCPは、信頼の問題でもあります。機器が最初に受け入れる応答が、すべてのトラフィックを通すルーターと、調べる名前をすべて変換するDNSサーバーを決めます。その応答を支配すれば、機器の行き先を支配できます。RFC 2131のセキュリティー節は、現在の形を「かなり安全性が低い」と、明確に述べています。UDPとIPへ直接重ねた設計であり、想定した機器に、パスワードやキーを持たせにくいためです。同じ節は、許可されていないサーバーを簡単に設置でき、誤ったアドレスや重複アドレス、なりすましのルーターやネームサーバーを渡せると記します。保護は、プロトコル自体ではなく、その周囲のネットワークで行う必要があります。

実際の活用例

ハードウェアアドレス00-00-5E-00-53-2AのノートPCが、オフィスのサブネット192.0.2.0/24へ入る例を考えます。192.0.2.1のマシンが、ルーターとDHCPサーバーを兼ねます。最初はアドレスがないため、送信元を0.0.0.0として、同じリンク上のすべての機器へブロードキャストします。四つのメッセージで、設定が完了します。

```
ノートPC 00-00-5E-00-53-2A              サーバー 192.0.2.1

1  DHCPDISCOVER  0.0.0.0 -> 255.255.255.255、サーバーポート67
                 ここにサーバーはありますか？
2  DHCPOFFER     192.0.2.50を86400 s間貸し出すと提示
                 サーバーID 192.0.2.1
3  DHCPREQUEST   ブロードキャスト：サーバーID 192.0.2.1
                 要求アドレス192.0.2.50
4  DHCPACK       192.0.2.50をノートPCへ86400 s間貸し出す
```

探索メッセージには、何台のサーバーが答えても構いません。クライアントは、複数の提示を集めるために待つこともできます。その中から一つを選び、サーバー識別子オプションで選んだ相手を示し、その相手が提示したアドレスを要求するメッセージを、ブロードキャストします。そのブロードキャストを受け取ったほかのサーバーは、自分の提示の拒否と見なします。選ばれたサーバーは、対応関係をストレージへ確定して保存し、確認応答を返します。

確認応答には、設定が入ります。各設定は、RFC 2132で番号を定めたオプションです。このノートPCには、たとえば次を渡せます。

```
オプション53   メッセージの種類      5（DHCPACK）
オプション54   サーバー識別子        192.0.2.1
オプション51   リース時間            86400（秒、一日）
```

```
オプション1   サブネットマスク      255.255.255.0
オプション3   ルーター              192.0.2.1
オプション6   DNSサーバー           192.0.2.53
```

RFC 2132は、サブネットマスクとルーターの両オプションがある場合、マスクを先に置くことを要求します。ルーターもネームサーバーも、優先順に複数並べられます。リース時間とサーバー識別子は任意ではありません。RFC 2131では、要求に対する確認応答に、両方が必須です。

192.0.2.50を使う前に、クライアントは、ARPなどで、ほかの機器がすでに使っていないか確認するべきです。使用中なら、DHCPDECLINEを送り、最初からやり直す必要があります。そうでなければ、タイマーが動き始めます。サーバーが独自の値を渡さない限り、T1はリースの半分、T2は八分の七です。一日のリースなら、次のようになります。

```
t = 0 s        DHCPACKを受信、リース開始
t = 43200 s    T1: RENEWING、192.0.2.1へDHCPREQUESTをユニキャスト
t = 75600 s    T2: REBINDING、任意のサーバーへDHCPREQUESTを
               ブロードキャスト
t = 86400 s    リース終了：192.0.2.50の使用をやめ、最初からやり直す
```

RFCは、同時に起動した部屋中のノートPCが、一度に更新しないよう、両タイマーの設定値に、ある程度ランダムな揺らぎを加えるよう求めています。応答がなければ、クライアントは、残り時間の半分を待って再試行します。待ち時間の下限は60秒です。正常なクライアントは、半分の時点で更新し、期限ぎりぎりにはなりません。

サーバーは、ノートPCと同じサブネットになくても構いません。ルーターをリレーエージェントにすると、ブロードキャストを受けて、別の場所のサーバーへ渡します。メッセージのgiaddrフィールドに記録した、リレー自身のアドレスが、応答の送り先を伝えます。RFC 2131も、この仕組みを前提とし、各ネットワーク区間にDHCPサーバーを置かずに済むと記しています。当社のネットワークとVPNのサービスのページは、1,000台のWi-Fiルーターの設定とデプロイ、1,000台を超えるサーバーのネットワーク基盤の管理を挙げています。この規模では、手でアドレスを入力する方法は使えず、プール、リース、リレーの配置も、ネットワーク設計の一部になります。

問題が起きるところ

不正なサーバーが、先に答えます。 誤った向きにつないだ家庭用ルーター、オフィスのネットワークへブリッジ接続したテスト機、意図的な攻撃者は、いずれもDHCPDISCOVERへ応答できます。プロトコルには、どれが正しいサーバーかを教える仕組みがありません。RFC 2131は、誤ったアドレスや重複アドレスを渡し、なりすましのルーターやネームサーバーへ向けられると列挙します。スイッチでフィルターできます。RFC 7610は、そのIPv4版であるDHCP snoopingが、広く導入されていると記しています。サーバーからのDHCPメッセージは、正規のサーバーやリレーにつながるスイッチポートだけで許可し、それ以外では破棄します。

プールが枯渇します。 アドレス数は固定で、動的割り当てで戻るのは、リースが終わるときです。数百台の携帯電話が出入りするゲストネットワークで、一週間のリースを渡すと、過去一週間に来た全員が、まだアドレスを持っています。RFC 2131は、悪意あるクライアントが、全アドレスを自分用に確保し、ほかのクライアントには一つも残さないようにできるとも警告しています。一回のリース期間中に存在する機器数に合わせてプールを設計し、出入りの多い場所では、リースを短くします。

新しいサブネットに、リレーがありません。 探索はブロードキャストで、ルーターを越えません。リレーエージェントを設定しない新しいVLANやオフィスの階には、応答が届きません。RFC 3927を実装したホストは、169.254/16から、リンクローカルアドレスを自分へ割り当てる場合があります。そのリンク内だけで使えます。ルーターは、そのアドレスを送信元や宛先とするパケットを転送してはいけないためです。DHCPクライアントのある各サブネットのルーターにリレーを設定し、クライアントの169.254アドレスは、サーバーが答えなかった手掛かりと見ます。

二台のサーバーが、食い違います。 耐障害性のために二台動かすのは合理的です。ただしRFC 2131は、どの提示を選んでも同じ動作になるよう、すべてのサーバーが、アドレス自体以外は同じパラメーターを返すべきだとしています。整合を保つ責任は、管理者に置きます。範囲が重なると、同じアドレスを二台に貸す可能性もあります。サーバーごとに別の範囲を与え、オプションは同じに保ち、変更のたびに両者を比べます。

固定アドレスを、プール内から選びます。 DHCPが貸す範囲内のアドレスを、手でプリンターに固定すると、いずれリースと衝突します。プロトコルは、検出を試みます。サーバーは、再利用する直前のアドレスを、ICMPエコー要求などで調べるべきです。新しいアドレスが使用中だと分かったクライアントは、必ず辞

退します。その後、サーバーは使用不可と記録し、管理者へ通知するべきです。これらは安全網で、設計の代わりではありません。手で設定するアドレスは、プール外に置くか、手動割り当てを使い、サーバー自身が予約を保持するようにします。

IPv6を、開いたままにします。 DHCPv4のフィルターは、別ポートで動くDHCPv6には効きません。ルーター広告がDHCPv6の利用を示すと、クライアントが開始する場合があります。RFC 9915は、不正なDHCPv6サーバーの対策として、RFC 7610、DHCPv6-Shieldを参照します。RFC 7610は、不正なルーター広告は対象外で、Router Advertisement Guardの仕事だとします。アクセスポートで、DHCPv4と同様にDHCPv6サーバーのメッセージをフィルターし、RA-Guardも併用します。

参考資料

- RFC 2131：Dynamic Host Configuration Protocol — プロトコル本体です。割り当て方式、リース、メッセージ交換、T1とT2のタイマー、セキュリティー節を含みます。
- RFC 2132：DHCPオプションとBOOTPベンダー拡張 — サブネットマスク、ルーター一覧、リース時間、メッセージの種類など、番号付きの全オプションです。
- RFC 9915：IPv6用Dynamic Host Configuration Protocol（DHCPv6） — IPv6のプロトコル、ポート、メッセージ、SLAACとの併用方法です。RFC 8415を置き換えます。
- RFC 7610：DHCPv6-Shield、不正なDHCPv6サーバーからの保護 — スイッチでのサーバーメッセージのフィルター、先行するIPv4のDHCP snooping、RA-Guardへ任せる範囲です。
- RFC 3927：IPv4リンクローカルアドレスの動的設定 — サーバーが答えないとき、ホストが自分に与える場合がある169.254/16のアドレスと、ルーターが転送しない理由です。

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

「DHCP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/dhcp/