

プライベートインターネット用のアドレス割り当て

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[プライベート アドレス領域](#)

[プライベート アドレス領域の使用の長所と短所](#)

[設計上の考慮事項](#)

[セキュリティに関する考慮事項](#)

[結論](#)

[関連情報](#)

概要

[このドキュメントは RFC 1597 に基づいており、ネットワーク内のプライベート ホストにグローバルに一意的な IP アドレスを割り当てずに、IP アドレス空間を節約するために役立ちます。この方法でも、ネットワークのすべてのホスト間およびインターネットのすべてのパブリック ホスト間で、十分なネットワーク レイヤ接続を実現できます。](#)

IP を使用するホストは、次の 3 つのカテゴリに分かれます。

- ほかの企業またはインターネット全体のホストへのアクセスを要求しないホスト。このようなホストは、ネットワーク内で一意な IP アドレスを使用できます。このアドレスは、外部ネットワークとの間で一意である必要はありません。
- アプリケーション レイヤ ゲートウェイによって処理できる（電子メール、FTP、ネットニュース、リモート ログインなどの）一部の外部サービスへのアクセスが必要なホスト。このようなホストの多くは、プライバシーまたはセキュリティ上の理由のために、（IP 接続によって提供される）無制限の外部アクセスを必要としない、または希望しないことがあります。最初のカテゴリのホストと同様に、このようなホストは、ネットワーク内では一意で、外部ネットワークとの間では一意でない IP アドレスを使用できます。
- IP 接続によって提供される企業外部へのネットワーク レイヤ アクセスを必要とするホスト。このようなホストだけが、グローバルに一意的な IP アドレスを必要とします。

多くのアプリケーションは、1 つのネットワーク内だけで接続を要求し、ほとんどの内部ホストでは外部接続を必要としません。大規模なネットワークでは、ネットワーク外部へのネットワーク レイヤ接続を必要としない場合に、ホストは TCP/IP を使用することがあります。次に、外部接続が必要とされない例をいくつか示します。

- TCP/IP によって個々にアドレス指定できる到着および出発ディスプレイを有する大きな空港

- 。このようなディスプレイに、ほかのネットワークからの直接アクセスが必要になることはほとんど考えられません。
- 内部通信のために TCP/IP を使用する銀行や小売チェーン店などの大きな組織。レジ、現金自動支払機、および事務員用の装置などの多くのローカルワークステーションに、外部接続が必要になることはめったにありません。
 - インターネットに接続するためにアプリケーションレイヤゲートウェイ (ファイアウォール) を使用するネットワーク。通常、内部ネットワークはインターネットに直接接続されません。このため、インターネットからは 1 台または複数のファイアウォールホストだけが可視になります。この場合、内部ネットワークには一意でない IP 番号を使用できます。
 - 独自のプライベートリンクを通じて通信する 2 つのネットワーク。通常、ごく一部のホストだけが、このリンクを通じて相互に通信できます。このようなホストだけにグローバルに一意な IP 番号が必要です。
 - 内部ネットワークのルータのインターフェイス。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

表記法

ドキュメント表記の詳細は、『[シスコテクニカルティップスの表記法](#)』を参照してください。

プライベートアドレス領域

Internet Assigned Numbers Authority (IANA) は、プライベートネットワーク用に、次の 3 ブロックの IP アドレス領域を予約しています。

- 10.0.0.0 - 10.255.255.255
- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255

最初のブロックは単一のクラス A ネットワーク番号、2 番目のブロックは 16 の連続するクラス B ネットワーク番号のセット、3 番目のブロックは 255 の連続するクラス C ネットワーク番号のセットです。

プライベートアドレス領域を使用することにした場合は、IANA またはインターネットレジストリと調整を行う必要はありません。このプライベートアドレス領域内のアドレスは、ネットワーク内だけで一意になります。グローバルに一意なアドレス領域が必要な場合は、インターネットレジストリからアドレスを取得する必要があることに注意してください。

プライベートアドレス領域を使用するには、外部へのネットワークレイヤ接続を必要としないホストを決定します。このようなホストがプライベートホストで、プライベートアドレス領域を

使用します。プライベートホストは、ネットワーク内のほかのすべてのホスト（パブリックおよびプライベートの両方）と通信できますが、外部ホストへのIP接続はできません。ただし、プライベートホストは、アプリケーションレイヤリレーを通じて外部サービスにアクセスできます。

その他のすべてのホストはパブリックで、インターネットレジストリによって割り当てられるグローバルに一意的なアドレス領域を使用します。パブリックホストは、ネットワーク内のほかのホストと通信したり、外部パブリックホストにIP接続することができます。パブリックホストは、ほかのネットワークのプライベートホストには接続できません。

プライベートアドレスにはグローバルな意味がないため、プライベートネットワークに関するルーティング情報は外部リンクに伝搬されず、送信元または宛先アドレスがプライベートなパケットは、外部リンクを通じて転送する必要がありません。特にインターネットサービスプロバイダーのルータなど、プライベートアドレス領域を使用しないネットワーク内のルータは、プライベートネットワークに関するルーティング情報を拒否（フィルタで排除）するように設定する必要があります。この拒否がルーティングプロトコルエラーとして処理されないようにします。

（DNSリソースレコードなど）このようなアドレスへの間接参照は、ネットワーク内に保持する必要があります。インターネットサービスプロバイダーは、このようなデータの漏出を防ぐための措置を取る必要があります。

プライベートアドレス領域の使用の長所と短所

インターネット全体でプライベートアドレス領域を使用することの明らかな長所は、グローバルに一意的なアドレス領域が節約されることです。また、プライベートアドレス領域を使用すると、ネットワーク設計での柔軟性が高まります。これは、グローバルに一意的なプールから取得できるよりも多くのアドレス領域を利用できるためです。

プライベートアドレス領域を使用することの主な短所は、インターネットに接続する場合に、自分のIPアドレスを覚えておく必要がある点です。

設計上の考慮事項

最初にネットワークのプライベート部分を設計して、すべての内部リンクにプライベートアドレス領域を使用します。次に、パブリックサブネットを計画し、外部接続を設計します。

使用する装置で適切なサブネット化スキームを設計およびサポートできる場合は、24ビットブロックのプライベートアドレス領域を使用し、適切な拡張パスでアドレッシング計画を作成します。サブネット化に問題がある場合は、16ビットクラスCブロックを使用できます。

ホストをプライベートからパブリックに変更するには、アドレスを変更し、ほとんどの場合、物理接続を変更する必要があります。（コンピュータールームなど）このような変更を予測できる場所では、変更を容易にするために、パブリックおよびプライベートサブネット用に、別個の物理メディアを構成できます。

外部ネットワークに接続するルータは、漏出を防ぐために、リンクの両方のエンドで適切なパケットおよびルーティングフィルタを設定する必要があります。プライベートアドレス領域へのルートが、ネットワークの外部を指している場合に発生することがあるあいまいなルーティング状況を防ぐために、プライベートネットワークで着信ルーティング情報にもフィルタを適用する必要があります。

相互通信が必要になると予測される組織のグループでは、共通のアドレッシング計画を設計する必要があります。外部サービスプロバイダーを使用して2つのサイトを接続する必要がある場合は、プライベートネットワークからのパケットの漏出を防ぐために、IPトンネルの使用を検討してください。

DNS RR の漏出を防ぐ1つの方法では、2つのネームサーバを実行します。一貫性を確保するために、両方のサーバは同じデータを受信し、外部ネームサーバはフィルタを適用したデータだけを使用します。

すべての内部ホスト（パブリックとプライベートの両方）のリゾルバは、内部ネームサーバだけにクエリーを実行します。外部サーバは、外部リゾルバからのクエリーを解決し、グローバルDNSにリンクされます。内部サーバは、企業外の情報に対するすべてのクエリーを外部ネームサーバに転送します。このため、すべての内部ホストは、グローバルDNSにアクセスできます。この方法では、プライベートホストに関する情報は、外部リゾルバおよびネームサーバには到達しません。

[セキュリティに関する考慮事項](#)

プライベートアドレス領域の使用によってセキュリティを向上させることができますが、専用のセキュリティ対策の代わりにはなりません。

[結論](#)

このスキームでは、多くの大規模ネットワークは、グローバルに一意なIPアドレス領域から比較的小さなアドレスのブロックだけを必要とします。インターネット全体では、グローバルに一意なアドレス領域が節約されるという利益が生じ、ネットワークでは、比較的大きなプライベートアドレス領域による柔軟性の向上という利益が生じます。

[関連情報](#)

- [IPルーティングプロトコルに関するサポートページ](#)
- [IPルーティングに関するサポートページ](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)