サイバーセキュリティ神話

導入

インターネットは過去数十年間で目覚ましい発展を遂げてきたものの、今日に至るまで依然として脆弱であり、大小さまざまな攻撃にさらされている。ユーザーはその複雑な仕組みを理解しておらず、侵入者によるハッキングと保護ソフトウェアの不具合を区別できない場合が多い。

最近の事例の一つとして、2025年11月18日にCloudflare社が世界規模のシステム障害に見舞われ、インターネットの大部分が一時的に機能停止に陥ったことが挙げられる[1]。これは単発的な出来事ではなく、その8ヶ月前にも同様の障害が発生しており、それ以前にも同様の事例が複数あった。同様に、Amazon Web Services（AWS）も頻繁にサービス停止に見舞われている[2]。このようなインターネット障害はもはや日常茶飯事となっており、サイバー攻撃からシステムを守るために設計されたこれらのサービスの信頼性が問われている。

問題

インターネットの脆弱性は数十年来の問題となっている。昨年、連邦通信委員会（FCC）は、リスク軽減の対象としてボーダーゲートウェイプロトコル（BGP）[4]を特定する規則制定案通知（NPRM）[3]を発表した。インターネットコミュニティを代表するインターネットアーキテクチャ委員会（IAB）は、これに対し懸念を表明する意見書[5]を提出した。それにもかかわらず、ホワイトハウスは、インターネットルーティングセキュリティ強化の手段としてBGPの整合性に焦点を当てたロードマップ[6]を公表した。

この点に関して、BGPは自律システム（AS）間[7]でパケットを転送するために必要であることを念頭に置いておくことが重要です。ドメインネームサーバー（DNS）[8]によって選択されるもの、ダイナミックホスト構成プロトコル（DHCP）[9]によって加入者に割り当てられたIPv4アドレスに基づいている。これはIPv4アドレス不足に対処するために開発されたものだ。このプロトコルスタックは、多くの側面から攻撃を受けやすい複雑なシステムアーキテクチャを生み出し、それぞれの攻撃に対して個別のパッチが必要となる状況となっている。

解決策

欠陥のあるシステムは、際限のないハッキングとパッチの適用を招きます。より堅牢なインターネットは、IPv4アドレス不足の根本原因を解消する、簡素化され合理化されたアーキテクチャによって実現できます。これにより、前述の4つのプロトコルのいずれも不要になります。このようなシステムは、EzIP[10]と呼ばれる決定論的なシステムによって実現されます。

テクノロジーとアーキテクチャの進化

インターネットが始まった当初、明確に定義された大規模な IPv4 アドレスブロックが、5 つの地域インターネットレジストリ（RIR）に割り当てられました。例えば、ヒルベルト曲線などです。[11]
以前の AFRINIC（アフリカ）、APNIC（アジア太平洋）、ARIN（北米）、LACNIC（ラテンアメリカおよびカリブ海地域）、RIPE（ヨーロッパ、中東、中央アジア）への割り当て状況は容易に識別できた [12]。

各地域インターネットレジストリ（RIR）は、割り当てられた IP アドレスをそれぞれの地域内のインターネットアクセスプロバイダー（IAP）に割り当てましたが、IAP 自体は同じ制限を遵守する必要はありませんでした。これにより、IP アドレスの断片化が急速に進み、加入者の物理的な所在地が、割り当てられた IP アドレスが最初に割り当てられた地域と地理的に一致しないという状況が生じました。

IPv4 アドレスプールの枯渇が始まったため、DHCP は利用可能なパブリック IPv4 アドレスを動的に再利用することで、インターネットアクセスプロバイダー（IAP）の運用を維持しました。その後、このような絶えず変化する環境下で加入者の負担を軽減するために DNS が導入されました。この 2 つのプロトコルは当時の差し迫ったニーズを満たしたため、インターネットの基本的な構成要素として定着しました。（この特異な組み合わせがもたらした影響については脚注を参照してください。）

初期導入機関が IPv4 アドレスプールの枯渇圧力を軽減するために、余剰の IPv4 アドレスブロックを公開オークションに出品することに同意したことで、IPv4 アドレスに意味のある物理的な位置情報が含まれていると期待することはもはや現実的ではなくなり、ましてや加入者の位置情報を特定することなど不可能になった。このニーズに応えるために、業界内に新たな分野が誕生した。しかし、その提供する情報の解像度と精度は、多くの場合、せいぜい疑わしいものだった [13]。

その過程で、1 つ以上の IPv4 アドレスブロックを所有するインターネットアクセスプロバイダー（IAP）は、それぞれ独自の IP パケット配信方式を開発しました。同じトランスポートポリシーを共有するアドレスブロックはグループ化され、1 つの自律システム（AS）を形成しました。各 AS の範囲は様々で、多くの場合限られているため、AS 境界を越えて IP パケットを転送するために BGP が利用されました。AS の数が増えるにつれて、BGP の複雑さも増大しました。これは、かなりの距離を移動するパケット、特にローカルネットワーク内を移動するパケットだけでなく、複数の AS 境界を越えてグローバルアドレス宛てに送信されるパケットにも当てはまります。

これらのプロトコルはそれぞれ本質的に分散型であるものの、その運用にはかなりの調整が必要であり、それが中央集権的な取り組みに依存しているため、Cloudflare や AWS などのコンテンツデリバリーネットワーク（CDN）[14] 事業者といった、限られた数の資金力のある企業が優位に立つ結果となっている。これらの企業は、インターネットの伝送インフラストラクチャの中核を担っている。

矛盾

インターネットには、その原理や仕組みを分かりにくくしている慣行が少なからず存在する。

インターネットは競争条件の均等化を促進する。しかし、バチカン市国は一人当たり21.4個のIPv4アドレスを割り当てられているのに対し、10数もの国や地域は割り当てがゼロで、その他の国々はその中間にあるあらゆる可能性の範囲内で割り当てを受けている[15]。
（注：セーシェルが 58.4 という配分を受けているのは異例であり、これは企業が地元の政治情勢を利用してグローバルなビジネスチャンスを獲得した結果である。）

インターネットはエンドツーエンドの接続性を約束していた。しかし、現在主流となっている運用モデルであるCDNは、たとえ地域コミュニティ内であっても、そのような目標の達成を阻害している。

インターネットは、通信会社の独占や公衆交換電話網（PSTN）に対する政府規制に異議を唱えて登場しました。しかし現在、インターネットは多国籍コングロマリットによって支配され、それぞれが事実上各事業分野を独占し、責任を無視したり規制を回避したりするまでになっています。このような中央集権化は、分散型インターネットという当初のビジョンに真っ向から反するものではないでしょうか？

また、約 200 もの世界各国の管轄区域がインターネットを分断し、地政学的な「スプリンターネット」[16]となる可能性についても、インターネットコミュニティから批判の声が上がっている。一方、AS（自律システム）は既にインターネットを少なくとも77,000層もの階層を持つオニオンネットワークに変えてしまっている[7]。さらに、ほとんどのAS（自律システム）は世界の特定地域のみにサービスを提供しているため、タマネギの皮の各層は、穴の開いた部分的な漁網のようなものと言えるでしょう。

最も不可解な点は、インターネットは国境のない原則を強く主張しているにもかかわらず、その主要なルーティングメカニズムはBGPへと進化しており、その「B」は各AS（自律システム）を取り囲む境界線を意味していることだ！

全体として、これらのプロトコルは非常に複雑で動的かつ分散型の性質を持っているため、インターネットは日常的な嫌がらせからランサムウェアに至るまで、幅広い悪意のあるセキュリティ侵害に対して脆弱になっている。

ここで述べておくべきなのは、IPv6 は自身の膨大なアドレス空間を十分に活用することなく、一時的なニーズから生まれた IPv4 の慣行を取り入れてしまったということである。そして今、IPv6 の重要性は静かに薄れつつあるように見える [17]。一方、IPv4 の廃止時期についてはもはや言及されなくなっている。IPv6 は IPv4 に比べて目立った利点を示していないため、現在進行中のインターネットに関する議論のほとんどでは、両者を区別することはなくなっている。

参考文献

1. Cloudflare 停電履歴(2019-2025)
https://controld.com/blothe/biggest-cloudflare-outages/

2. AWS クラウドおよびデータセンターの障害履歴
https://www.datacenterknowledge.com/outages/a-history-of-aws-cloud-and-data-center-outages

3. ボーダーゲートウェイプロトコル（BGP）のリスク軽減対策の進捗状況に関する報告。安全なインターネットルーティング
https://www.federalregister.gov/documents/2024/06/17/2024-13048/reporting-on-border-gateway-protocol-risk-mitigation-progress-secure-internet-routing

4. ボーダーゲートウェイプロトコル
https://en.wikipedia.org/wiki/Border_Gateway_Protocol

5. インターネットソサエティ、インターネットアーキテクチャ委員会、およびインターネット名称割り当て機関（ICANN）による、「ボーダーゲートウェイプロトコル（BGP）のリスク軽減の進捗状況に関する報告」に関する意見書
https://datatracker.ietf.org/doc/statement-iab-comments-of-the-internet-society-internet-architecture-board-and-internet-corporation-for-assigned-names-and-numbers-in-the-matter-of-reporting-on-border-gateway-protocol-risk-mitigation-progress/

6. インターネットルーティングセキュリティ強化のためのロードマップ
https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/09/Roadmap-to-Enhancing-Internet-Routing-Security.pdf

7. 自律システム（インターネット）
https://en.wikipedia.org/wiki/Autonomous_system_(Internet)

8. ドメインネームシステム
https://en.wikipedia.org/wiki/Domain_Name_System

9. 動的ホスト構成プロトコル
https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol

10. 決定論的なインターネット
https://avinta.com/gallery/DeterministicInternet-SPKR.pdf

11. ヒルベルト曲線
https://en.wikipedia.org/wiki/Hilbert_curve

12. ヒルベルト曲線を用いて IPv4 アドレス空間を視覚化する
https://thebayesianobserver.wordpress.com/2011/10/23/121/

13. インターネットジオロケーション
https://en.wikipedia.org/wiki/Internet_geolocation

14. コンテンツ配信ネットワーク
https://en.wikipedia.org/wiki/Content_delivery_network

15. IPv4 アドレス割り当てによる国別リスト
https://en.wikipedia.org/wiki/List_of_countries_by_IPv4_address_allocation

16. スプリンターネット
https://en.wikipedia.org/wiki/Splinternet

17. ジェフ・ヒューストン：インターネットの過去、現在、そして未来
(TM: 1:08:18, 「IPv6 — ますます重要性が薄れている」)
https://cloudflare.tv/this-week-in-net/geoff-huston-the-internet-s-past-present-and-future/dg78lmvO

脚注

DHCP と DNS は、長年にわたり誰もが当たり前のように使ってきたにもかかわらず、最も理解しにくいインターネット技術の組み合わせと言えるでしょう。DHCP は、必要に応じて加入者に IP アドレスを動的に割り当てることで個人のプライバシーを保護すると謳っていますが、実際には、DNS が要求に応じて、対象となる相手の識別情報に基づいて、その相手に割り当てられた最新の IP アドレスを即座に提供してしまうため、そのプライバシー保護は完全に無効化されてしまいます。これにより、一般ユーザーは保護されているという誤った安心感を抱き、まるで砂に頭を突っ込んだダチョウのような状態に陥る一方、多くの IT エンジニアはこうした仕組みのおかげで安定した職を得ています。これはまさに中国の故事成語「矛盾」の完璧な例と言えるでしょう。

それにもかかわらず、この仕組みに基づいたプロトコルの層が AS や BGP を経て積み重ねられ、多国籍企業の支配を可能にする CDN が構築され、さらに Cloudflare や AWS といった主要サービスへと発展していきました。これらのサービスは、セキュリティを強化した信頼性の高いパケット伝送を提供することを謳っていました。しかし、これらのサービスの堅牢性はしばしば疑問視されてきました。そして、インターネットが侵害された際、誰も責任を負おうとせず、脆弱性を軽減するための代替策を探そうともしませんでした。おそらく、インターネット全体があまりにも分散化されていたため、責任の所在を特定することが困難だったのでしょう。

一方、現在のインターネット構成は、攻撃者にとって理想的な環境となっている。攻撃者は、任意の架空の IP アドレスを正当な一般インターネット加入者として偽装し、攻撃を開始した後、痕跡を残さずにそれを放棄することができるため、法医学的な追跡調査に役立つ有効な身元情報を含む永続的な記録はほとんど残らない。