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。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。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）を特定する規則制定案通知（NPRM）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を公表した。

この点に関して、BGP は自律システム（AS）間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）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）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 と呼ばれる決定論的なシステムによって実現されます。

(ぜひお越しください https://avinta.com/gallery/CyberSecurityMyth-JP.pdf 全文はこちら.)