エグゼクティブサマリー

サイバーセキュリティ神話：

なぜ段階的な修正では不十分なのか、そして EzIP がよりシンプルで安全な解決策を提供する理由

インターネットは現代社会を支える基盤ですが、依然として脆弱性を抱えています。2025 年 11 月に発生した Cloudflare の世界的規模の障害や、Amazon Web Services で頻繁に発生するサービス停止は、セキュリティと信頼性の向上を目指して設計された大手プロバイダーであっても、依然として脆弱性が存在することを浮き彫りにしています。連邦政府の取り組み（FCC の規則制定案、2024 年）やホワイトハウスのインターネットルーティングセキュリティ強化ロードマップ（2024 年）は、より強力な監視と検証のためにボーダーゲートウェイプロトコル（BGP）を対象としています。これらの措置は有益ですが、より根深い問題、すなわち IPv4 アドレスの当初からの不足という問題の症状に対処しているに過ぎません。限られたアドレス数に対処するために、以下の対策が講じられています。

• 動的割り当て（DHCP）により、IP アドレスは一時的なものとなった。
• DNS がこれらの変更を追跡した。
• ネットワークは数千ものドメイン（自律システム）に分割され、それらを接続するために BGP が利用された。
• コンテンツ配信ネットワーク（CDN）は、複雑さを管理するためにトラフィックを集中させた。

この構成は混乱、単一障害点、そして攻撃者にとって有利な状況を生み出します。偽装されたアドレスは簡単に使用でき、追跡が困難である一方、正規ユーザーは明確な記録を残してしまいます。集中型 CDN は格好の標的となり、パッチ適用は根本原因を解決することなく、さらに複雑な層を追加するだけです。EzIP（Easy IPv4）は、長年予約されていた IPv4 240/4 ブロックを再利用することでこの問題を解決し、数百万の拠点に固有の静的パブリックアドレスを提供します。これにより、動的な再割り当てや問題のあるプロトコルへの過度な依存なしに、地域全体をカバーするのに十分なアドレスを提供できます。主な利点：

• より強力な固有セキュリティ — 静的アドレスにより、なりすましを検知しやすくなり、追跡可能性が向上し、設計上、攻撃対象領域が縮小されます。
• 信頼性の向上 — 複雑性の軽減により障害リスクが低減され、正確な地理位置情報が管理と対応を支援します。
• 最小限の混乱 — 既存のインターネット上にオーバーレイされ、強化された地域ルーターを介して段階的に展開されるため、大規模なデバイスのアップグレードは不要です。
• より広範なメリット — 中央集権化のリスクを軽減し、インターネットアーキテクチャを改善し、法執行機関による犯人特定を支援します。

EzIP は、インターネットを脆弱にしていた根本的な資源不足の問題に対処することで、IPv6 や既存のツールを補完します。これは、より強靭で公平なデジタルインフラの構築という目標にも合致するものです。詳細な分析については、以下のリンクをご覧ください。

https://avinta.com/gallery/CyberSecurityMyth-JP.pdf

によって準備された：Abraham Y. Chen / Avinta Communications, Inc.
接触：AYChen@Avinta.com / +1(650)248-1829
2026 年 1 月