2022.6

IPv6 とセキュリティ

＜目次＞

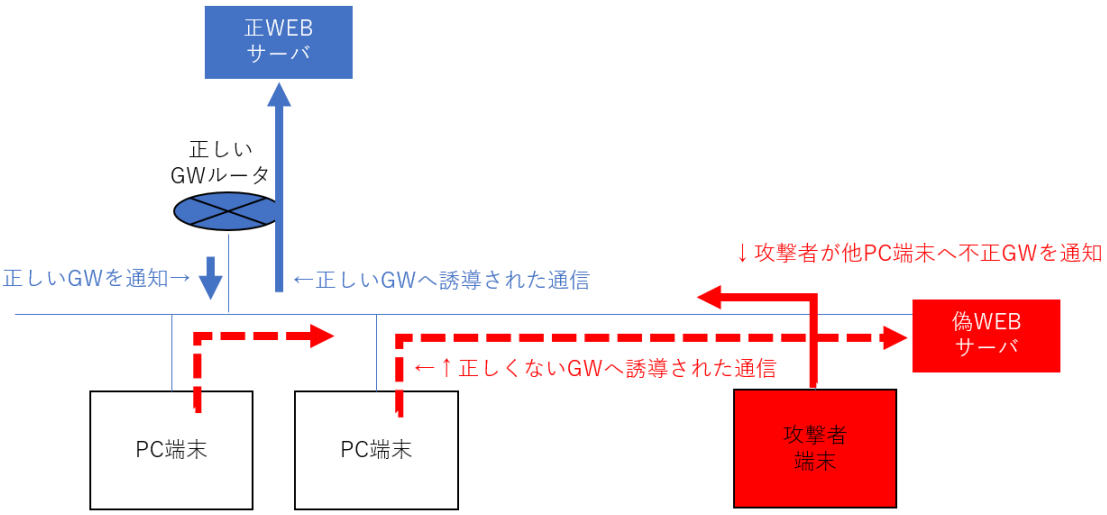
1. IPv6 について

IPv6 は、PC・タブレットなどの端末に対して、グローバルな IP アドレスが直接割り当てられる。インターネット上の外部端末から直接アクセスが可能となる為、通信機器のフィルタ機能などによって通信を保護する必要がある。

2. IPv6 における主な攻撃手法

2-1. 不正 RA（Router Advertisement）による盗聴

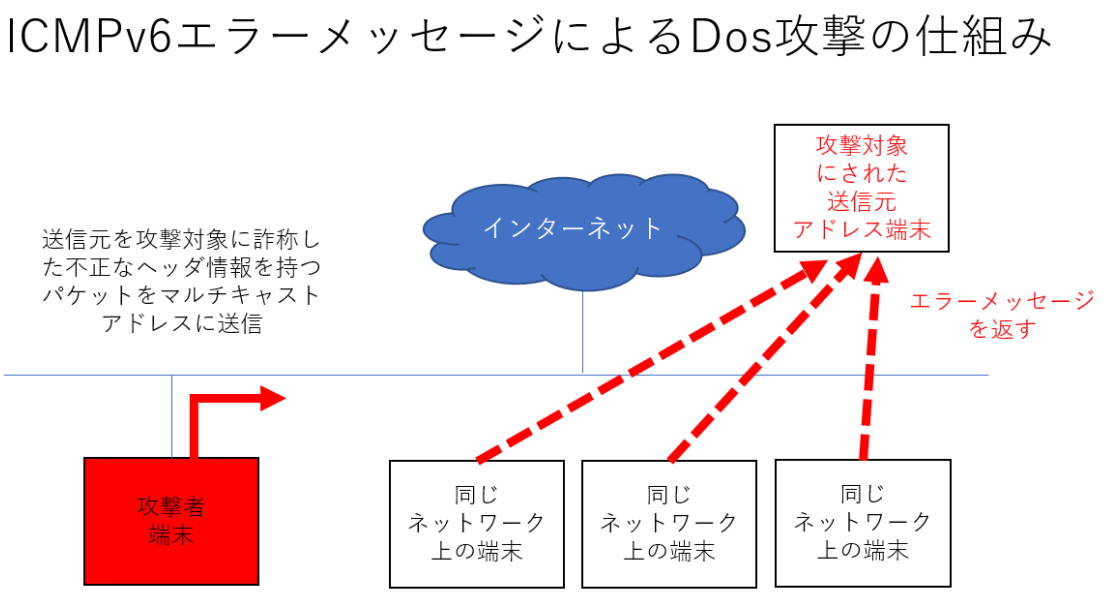
不正RAの仕組み



RA は、ルータが同ネットワーク内の機器に自分の存在を知らせるとともに、インターネットに関する情報や経路を広告する仕組みである。

不正 RA とは、正規の RA を偽装して、同ネットワーク上にある端末に対し、ブロードキャストで不正なデフォルトゲートウェイを通知する。それにより、通知を受け取った端末は不正なデフォルトゲートウェイへ誘導される事で、正常な通信ができなくなってしまう。

2-2. ICMPv6 エラーメッセージによる Dos 攻撃



IPv6 で使用されるプロトコルである ICMPv6 の仕様では、各 PC などの端末は問題のあるパケットを受信した際に「Parameter Problem」というエラーメッセージを、送信元のアドレスに返す。

ICMPv6 パケットを送っている送信元がマルチキャストアドレスの場合には、エラーメッセージを返さない仕様ではあるが、定められた特定のエラーに関しては返す仕様となっている。

この仕組みを悪用した手段として、下記の方法が存在する。

攻撃者端末は ICMPv6 パケットの送信元アドレスを攻撃対象に偽装した、特定の問題を内包したマルチキャストを発信する。

そうすると同ネットワーク上にある端末が、一斉に攻撃対象となった偽装された送信元アドレスにエラーメッセージを返す。

上述より攻撃対象となった端末に大量のパケットが届くため、攻撃対象となった端末のネットワーク帯域やＣＰＵなどの資源に影響を及ぼす Dos 攻撃を受ける可能性がある。

3. 必要なセキュリティ対策

3-1. ルータでの対策

＜ND Proxy 機能の有効化＞

IPv6 対応ルータには、ND Proxy と呼ばれる IPv6 のパケットを直接、PC などの端末に配送するのではなく、ルータを介して配送するモードがある。
送受信される通信パケット情報を読み取り、あらかじめ設定されたルールに基づいて、外部から送信された受信パケットの通過を許可するかどうかの判断を行う。
IPv6 ファイアウォールのパケットフィルタリング機能の一つであり、有効化することで通信の安全性が高まる。

※NCT がレンタル品として提供する D-ONU は「パススルー」の為、IPv4/v6 共にパケットを素通しする。

◆ND とは

同ネットワーク上の通信には MAC アドレスを通信先情報として使用される。異なるネットワークのインターネット上では、IP アドレスを通信先情報として使用される。
同じネットワーク上で通信する際には、IPv4 では通信先の MAC アドレスを取得する為に ARP と呼ばれるプロトコルを使用しているが、IPv6 では「近隣検索（ND：Neighbor Discovery）」と呼ばれるプロトコルを使用する。
同ネットワーク上の IPv6 端末は、ND プロトコルを用いて IPv6 アドレスから MAC アドレスを取得し、それ以降は MAC アドレスを使って通信する。

◆ND Proxy 仕組み

ND Proxy 機能を有効化すると、外部から受信した IPv6 パケットは、ルータ等の ND Proxy まで配送され、そこから PC などの端末へ配送される。この時に、ND Proxy では受け取った通信パケット情報に不正が無いかを確認し、問題のないパケットであれば（フィルタルールに基づく）PC などの端末へ通信パケットを配送する。

＜IPv6 ファイアウォール機能の有効化＞

IPv6 対応ルータの中には、IPv6 ファイアウォール機能を搭載しているものがある。この機能はインターネット側(WAN)から内部端末側（LAN）への接続要求を拒否する機能である。
有効にすることでインターネットからの不正アクセスから端末を守ることに有効。
ND Proxy と機能は類似しているが、動的にフィルタルールを生成するなど、厳密には違う。

3-2. 端末での（PC、IoT など）対策

＜Windows 標準ファイアウォール機能の有効化＞

Windows に標準で搭載されているセキュリティ機能を有効化することで、不正なアクセスから保護（不正なアクセスを拒否）する事が可能。

ただし、適切な設定がなされていないと不正アプリケーションが通信を許可してしまう可能性があるため過信は禁物である。

＜セキュリティ対策ソフトに付属するファイアウォール機能を利用＞

上述と同様のファイアウォール機能を利用して、不正なアクセスから保護（不正なアクセスを拒否）する事が可能。セキュリティ対策企業が作成しているため、脆弱性の発見時はより迅速な対応が可能。

ただし、こちらも適切な設定がなされていないと不正アプリケーションが通信を許可してしまう可能性があるため過信は禁物である。

以上