

# Arp flood

分類            Arp DoS  
再現性         リモート

## 技術解説

### 1)概要

arp (Address Resolution Protocol) パケットを大量に送信することにより、ローカルネットワーク及びターゲットホストに使用不能状態を引き起こす攻撃である。

### 2)原因

大量の arp パケットを送信することにより、下記のような現象が発生する。結果として、ローカルネットワーク及びターゲットホストの使用不能状態が発生する。

- 大量の arp パケットが送信されること自体、トラフィックの増大によるネットワークへの過負荷の原因となり得る。
- ターゲットホストが、膨大な arp を受信することにより、処理を行う CPU に過負荷がかかってしまう。
- ターゲットホストの OS に arp テーブルに登録される arp 情報の件数制限がない場合、膨大な arp を受信すると、arp テーブル処理のために CPU に過負荷がかかってしまう。

## 影響

膨大な arp reply パケットを受けたターゲットマシンは、CPU 使用率が100%に達し、サービス不能状態に陥る。更に継続してパケットを受信すると、アプリケーションの一部が破損する可能性がある。

ただし影響を受けるのは、通常ローカルネットワーク上のホストに限られる。また CPU が過負荷状態になるのは、パケットを受信している間及び、攻撃による膨大な量の arp 情報を arp テーブルに表示する場合 (=arp.exe が実行された場合) のみである。膨大な量の arp キャッシュは、タイムリミットを過ぎると消去される。(Windows2000 の場合であれば、再利用されない限り 2 分で消去される)

## 影響を受けるOS、サービス

影響 ○:脆弱性あり、×:脆弱性なし

(2001/8/24現在)

OS	サービス	影響	備考
全ての Windows	arp	○	
Windows 以外の OS	arp	○※1	

※1 具体的にどのOSが影響を受けるかについての資料はなく、あくまで可能性であ

る。

OS Microsoft Windows (Windows以外の OS も影響を受ける可能性有り)  
サービス arp

## 対策方法

### 1)対策

有効な対策は、現在のところ特にない。( 2001年8月24日現在)

---

Copyright © 2002 警察庁