不正アクセス対策まとめ

ネットワーク上の脅威 (攻撃/不正アクセス)	分類	概要	対策方法	対策機能	効果
MAC flooding attacks	パケット盗聴	スイッチのFDB (Forwarding Database) を枯渇させる事により、フレームをフラッディングさせて盗聴を行う攻撃手法	FDBを枯渇させる不正なフレームを破棄	ポートセキュリティー	MACアドレス学習数の上限を設定することにより、FDBを枯渇させる不正なフレームを破棄することが可能
				IEEE802.1X (Single Host)	認証済み端末 (1ポート＝1端末) のみFDBに登録されるため、FDBを枯渇させる不正なフレームを破棄することが可能
DHCP starvation attacks	DoS	不正なDHCPパケットを送信してDHCPサーバーから多数のIPアドレスを取得し、DHCPサーバーのIPアドレスプールを枯渇させる攻撃手法	DHCPサーバーのIPアドレスプール枯渇させる不正なパケットを破棄	ポートセキュリティー	MACアドレス学習数の上限を設定することにより、IPアドレスプールを枯渇させる不正なDHCPパケットを破棄することが可能
				DHCPスヌーピング	DHCPクライアント数の上限を指定する事で、IPアドレスプールを枯渇させる不正なDHCPパケットを破棄することが可能
				IEEE802.1X	認証済み端末 (MACアドレス) からのパケットだけを転送するので、IPアドレスプールを枯渇させる不正なDHCPパケットを破棄することが可能
DHCP rogue server attacks	マン・イン・ザ・ミドル (盗聴、改ざん)	不正なDHCPサーバーを構築し、不正なGateway IPアドレスやDNSサーバーの情報をクライアントに割り当て、通信を行う二者の間に割り込む事で盗聴や改ざんなどを行う攻撃手法	正規なDHCPサーバーからのDHCPパケット (68/udp：宛先ポート) だけを許可する	DHCPスヌーピング	Untrustedポート (クライアントポート) からの68/udp (宛先ポート) は破棄されるため、不正なDHCPサーバーを排除することが可能
				ハードウェアパケットフィルター	正規なDHCPサーバーからの68/udp (宛先ポート) だけを許可することで、不正なDHCPサーバーを排除することが可能
IP address spoofing	なりすまし	IPアドレスの詐称を行い、アクセスリストなどのセキュリティ機能を回避して不正アクセスを行う攻撃手法	送信元IPアドレスの詐称を防止し、不正アクセスを阻止	DHCPスヌーピング	DHCPサーバーから正しくIPアドレスを取得した端末からのみ通信が行える仕組みのため、IPアドレスを詐称したパケットを破棄することが可能
				ハードウェアパケットフィルター	ハードウェアパケットフィルターにより送信元のIPを制限することで、IPアドレスを詐称したパケットを破棄することが可能
ARP poisoning attacks	マン・イン・ザ・ミドル (盗聴、改ざん)	不正なARPパケットを送る事で端末のARP情報を更新させて通信に割り込み、盗聴などを行う攻撃手法	不正なARPパケットの破棄	DHCPスヌーピング	ARPセキュリティオプションを利用する事で、不正なARPパケットを破棄することが可能