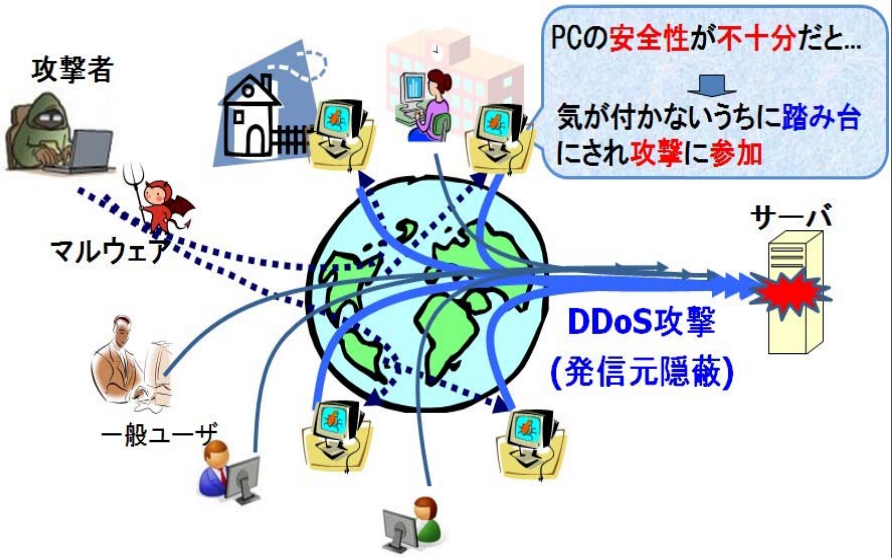
サイバー攻撃（DDoS攻撃）対策手法
Distributed Denial of Service Attacks Prevention Methods

★サイバー攻撃とは

金銭などの目的で，大企業や官公庁などのWebサーバへ大量のデータを送信し， Webサーバ（Webサイト）を利用できないようにするDDoS（サービス不能，サービス拒否）攻撃の被害が深刻な問題なっています．
しかし，実際にこれらの攻撃を行っているのは，ウィルスに感染された一般ユーザのPCが踏み台に利用されている場合が多いです．



★現状のサイバー攻撃対策

多くのインターネットサービスプロバイダーでは，バックボーンネットワークに専用のDDoS対策装置を設置し，通信量などの異常を検知したら，代理応答しながら帯域制御を実施していますが，攻撃者の発信元を明確に判断できないため，攻撃ではない通信も遮断されてしまいます．

★サーバ側とユーザ側のマルチ対策手法

【サーバ側での対策】

攻撃者のセッション確立時間と更新時間の間隔を記録し，攻撃として判断した場合，仮想Webサーバ（おとりサーバ）へ誘導します．
そして，おとりサーバへアクセスした攻撃者のIPアドレスを記録し，連続アクセスした場合，通信を遮断します．

【ユーザ側での対策】

一般ユーザのPCが攻撃者の呼びかけに応じて攻撃を行っている場合，エラーWebページを見せることで，自分が攻撃者の踏み台になっていることに気付かせることで攻撃を遮断します．