平成28年12月14日　長崎新聞　ふるさと総合面掲載

県立大・連続セミナー　5

ネットワークセキュリティ

侵入前提の対策必要

情報システム学部
情報セキュリティ学科教授
加藤　雅彦

私たちがいろんな手段で離れた相手とコミュニケーションをとるのと同じように、コンピューターもさまざまな手段を使って通信を行います。通信装置は、小包のようにして情報の塊を運びます。これを「パケット」と言います。荷札となる「パケットヘッダ」には、住所の代わりに「IPアドレス」という宛先を使います。

通信の信頼性とは、パケットが届いたことを確認するかしないかで、前者はWWWやメール、後者は動画の配信などに利用されています。宛先に届いたパケットはどうなるでしょうか。パケットには品名となる番号「ポート番号」がついており、この番号を見てコンピューターは受け取ったデータを、適切なアプリケーションを使って処理します。

ネットワークで情報を守るには、不正な通信を見つけて止める機器が必要です。代表的なものに「ファイアウオール」があります。これはパケットヘッダを見て、許可されているパケットなら通し、許可されていないパケットは通さない機能があります。

不正とする通信パターンを事前に定義しておき、それと一致する通信を見つけて遮断する機能を持っているのが「IPS」や「WAF」などです。一度に大量の通信がきたら攻撃とみなして捨てる、届いた情報を仮想システムで動かし、利用者と同様の操作を自動で行うことで不正な通信を判断する装置もあります。

しかし近年の攻撃は巧妙化しており、ネットワークの機能だけで不正な通信を判断し、攻撃を防ぐのは限界があります。個人でも企業でも、ネットワークに侵入される前提でセキュリティー対策を取る必要があります。

（次回掲載は21日です）