

研究テーマ：ネットワークセキュリティの調査

1, まえがき

私たちの普段使うネットワークには、外部からの攻撃を受ける危険性が存在する。その危険から、情報を守る技術のことをネットワークセキュリティと呼ぶ。

2, 研究課題

現在使われている、ネットワークセキュリティの技術を調査することで、その内容を理解する。

3, 研究結果

セキュリティ技術はそのOSI階層によっていろいろあるが、その中でもネットワーク層に用いられる「IPsec」、トランスポート層で用いられる「SSL」について調査した。

IPsecはAH・ESPというプロトコルを使用することによって、データ送信の際に、第3者によるなりすましを防ぎ、データを暗号化し、安全を確保する。

SSLは機能を大きく2種類に分けることができる。1つはSSLロードプロトコルというデータを暗号化し、メッセージ認証コードをつけ送信する。もう一つのグループは、サーバー間との暗号を更新する暗号更新プロトコル・警告を知らせてくれるプロトコル・データ通信に使われるプロトコルによって構成される。

3, 考察

IPのように、通信経路が決められていない場合と、SSLは下図のようにホストサーバー間が決まっている場合で、セキュリティにも違いがあることが分かった。大まかに見ると機能は似ていると思った。