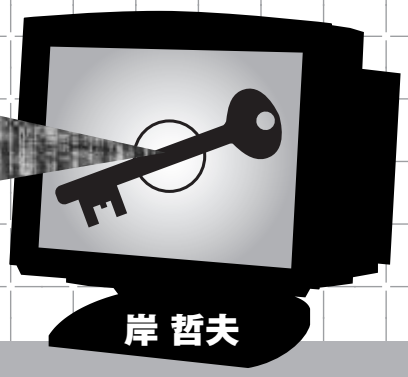
組み込みネットワーク機器のセキュリティを向上する

IPsecによる暗号化通信の実装（前編）



岸 哲夫

かつてインターネットは，学術用途の相互扶助ネットワーク的な役割であったため，インターネット上に流れるデータは暗号化されていなかった．しかし現在のインターネットは，金銭を取り扱う情報や個人情報，企業の機密情報などの交換にも使われ，データ通信の暗号化に対する要求が高まっている．ここでは，データ通信の暗号化を行うためのしくみであるIPsecをLinuxカーネル2.6で利用するための手順について解説する．（編集部）

1．平文と暗号文

● 基本的にネット上のデータは平文である

ネット上のデータを盗むことは比較的簡単です．普通の文章で書かれたものを受け渡ししているだけだからです．ネット上で受け渡されている，何も暗号で加工されていないデータ，それを「平文（へいぶん）」と呼びます．平分は「暗号文」の対義語で，これで受け渡しデータを送受信するプロトコルとして，POP，FTP，telnetなどが知られています．

● 暗号鍵とは何か――公開鍵と秘密鍵

データを盗まれないように，意図的に受け渡しのデータを暗号化してPOP，FTP，telnetなどで受け渡す場合もあります，復号には「暗号表」として「鍵」を配布します．

鍵の方式には2種類あります．一つは開ける鍵で，閉める鍵の対になる二つの鍵を使う「公開鍵暗号」です．もう一つは，どちらにも同じ鍵を用いる「秘密鍵暗号」です．

公開鍵暗号とは，公開鍵・秘密鍵の鍵ペアを利用する暗号化方式で，公開鍵で暗号化したデータは秘密鍵でしか復号することができず，秘密鍵で暗号化したデータは公開鍵でしか復号できないという特徴をもちます．

例えば，暗号文の送信などを行う場合には，あらかじめ送信相手の公開鍵をもらっておき，秘密文書を相手の公開鍵で暗号化します．受信者は，自分の秘密鍵で復号し，正しく情報が伝わることになります．秘密鍵は本人しか知らないという運用をするので，他人が暗号文を入手しても復号化できないから読めないよ，というものです（**図1**）．

一方，秘密鍵暗号は暗号化と復号に同じ鍵を用いる暗号方式です．開ける鍵も閉める鍵も同じ管理をします．こちらは鍵をコピーされたらおしまいです．とりあえず暗号化すれば文書を盗人に盗まれても解析が簡単にはできません．が，開ける人はいるし，解析するソフトウェアもあります．だからといって，データごとに鍵を変えていては不便な上に，どの鍵かを管理できずに混乱するでしょう．

2．IPsecの登場

● IPsecによるデータ通信とは

コンピュータ化する以前の文書の受け渡し方式に，パイプ中のカプセルに文書を詰めて圧縮空気で受け渡すという，メインテナンスがとても大変そうなシステムがありました．その通信パイプをいじられたらデータ盗人の天国になってしまいます．

逆に，そのパイプが絶対いじれず加工できないものならデータの受け渡しも安全です．たとえて言えば，パイプ・システムがインターネット（インターネット・プロトコル）で，パイプの中のカプセルがTCP/IPで，その中のPOPカプセルの中に手紙がある状態です．

このような暗号化を実現するためにIPsecが登場しました．IPsecは，パイプの中のものすべてに共通の鍵をかけると思って差し支えありません．パイプならば，1本のパイプが発信元と受信元を仮想的に接続した場合，これが「インターネットVPN」になります．ようするにパイプ自体が秘匿され，まるで専用線のように使うことができます（**図2**）．なお，トランスポート・モードではパケット・データ部のみを暗号化します．パイプの中のものすべてに共通の鍵をかけて流通している状態です．トンネル・モードは，パイプ自体が秘匿されたものです．

● IPsecは複数の暗号化方式を選択できる

IPsecは同一ノード間の通信においても，プロトコルや

本部からのメッセージ
「Aはスパイだ，査問せよ」

暗号化システム

暗号化された本部からのメッセージ
「nilke，shaozhajle;lahka」

メッセンジャBが運搬
しかしメッセンジャBは鍵を持っているので盗み読む
大変だとAに連絡

C → D → G
　 E → H
　 F → I
　　 → J

上のようなルートで暗号文は伝わる

なに？Bもスパイ？

すでに全員に配った鍵を変えなくては…

B　E　H
C　F　I
D　G　J

（**a**） 秘密鍵暗号とは

公開鍵　何らかの方法で公開するのでみんなが知っている
A→鍵生成アルゴリズム秘密鍵　当人以外は知らない

公開鍵　何らかの方法で公開するのでみんなが知っている
B→鍵生成アルゴリズム秘密鍵　当人以外は知らない

公開鍵　何らかの方法で公開するのでみんなが知っている
C→鍵生成アルゴリズム秘密鍵　当人以外は知らない

公開鍵　何らかの方法で公開するのでみんなが知っている
D→鍵生成アルゴリズム秘密鍵　当人以外は知らない

公開鍵　何らかの方法で公開するのでみんなが知っている
E→鍵生成アルゴリズム秘密鍵　当人以外は知らない

Bに暗号を送りたいAはBの公開鍵で暗号化した文書をBに渡す．Bは秘密鍵で復号する
以下C，D，Eに暗号文を送る

Bが怪しいとわかったらBの公開鍵で暗号を作ることをやめればよいだけ

暗号サーバ

←A　サーバに登録済みの全員の公開鍵で暗号文を送る（Bの公開鍵は削除する）
→B　各自の秘密鍵で復号する．え？失敗する？
→C　各自の秘密鍵で復号する
→D　各自の秘密鍵で復号する
→E　各自の秘密鍵で復号する

↑
RSA 暗号通信

しかし，大量のデータをやり取りする上でパフォーマンスに問題が出るため，IPsecの暗号化通信は秘密鍵を使用する
鍵の配布には「鍵交換」プロトコルを使用し，より安全に運用する

（**b**） 公開鍵暗号とは

図1　暗号のしくみ

発信元　ABCD
↓
インターネット　→　盗聴者　ABCD
↓
受信元　ABCD

盗聴者：なるほど例の暗号はABCDなんだな

（**a**） 平文によるデータ通信

発信元
↓郵便・メール便，実際にあって「暗号を開ける鍵」を渡す
送信元

（**b**） 暗号文によるデータ通信（秘密鍵暗号方式）

ABCDを発信
↓
ABCDを暗号化→WNBS
↓
インターネット　→　盗聴者　WNBS
↓
WBBSを事前に受け渡した鍵束で暗号解読→ABCD
↓
受信者：ABCD

盗聴者：WNBSってなんだ？
この鍵で開けると→ABCD

（**c**） 暗号化した後にメールでデータ通信

発信元
↓鍵交換プロトコルで「秘密鍵」を渡す
送信元

パソコン上からABCDを発信

ABCDを箱に入れて「鍵」をかける

インターネットで通信　盗聴者：インターネットで盗聴
↓
受信元は　秘密鍵で箱を開けてデータを取り出す

盗聴者：箱が開かない

（**d**） IPsecによるデータ通信（秘密鍵）

図2　IPsec の図式

ポート番号などによって複数の暗号化方式や暗号鍵，セキュリティ・プロトコルを使用できます．

こういった用途で双方で共有するパラメータをSA（Security Association）といい，SAを管理するデータベースをSADといいます．どのプロトコルでどのSADを使うかを決めるのが，SP（Security Policy）で，SPを管理するデータベースがSPDです．

エンコードされたIPsecヘッダ（AH・ESP）には所属するSAを示す32ビットのID情報が付加され，これをSPI（Security Parameters Index）と呼びます．SPIは暗号化通信で各パケット中に挿入され，パケット内の通信内容がどのような暗号化アルゴリズムで暗号化されたのか，どの暗号鍵を使うのかといったことを示すガイドとなります．