Camellia を使用した Linux カーネル, IPsec-tools のコンパイル方法

日本電信電話株式会社

Version 1.0, 2006 年 11 月 8 日

(1) Linux カーネルソースと『Linux-2.6.18 系への Camellia 追加パッチ』の取得

ftp.kernel.org などから linux-2.6.18.tar.bz2 をダウンロードします。

『Linux-2.6.18 系への Camellia 追加パッチ』を当 HP からダウンロードします。ダウンロードしたファイルを camellia-linux-2.6.18.patch.gz とします。

(2) Linux カーネルソースへのパッチ

$ tar xvfj linux-2.6.18.tar.bz2

$ cd 展開したディレクトリ

$ zcat ../camellia-linux-2.6.18.patch.gz | patch –p0

(3) Linux カーネルのコンパイルとインストール

下記のコマンドを入力し、Linux カーネルをコンパイル、インストールします。なお、環境によりコマンド、パラメータ等が異なる場合がございますので、適宜ご使用の環境に合わせて下さい。また、コマンドの詳細についてはマニュアルなどをご参照下さい。

$ make menuconfig

(3.1)表示されたメニューで、"Load an Alternate Configuration File"の項目を選択し、現在動作中のカーネルの config ファイルをロードします。

※ 使用中のカーネルのバージョンは、下記のコマンドで確認できます。

$ uname －a

上記コマンドの結果が、2.6.9-34.EL だった場合、/boot/config-2.6.9-34.EL のように設定します。

(3.2)Camellia を使用できようにするために、以下項目を選択します。

Cryptographic options ---->

次に、表示された項目の中の以下の項目を選択し、有効にします。

Camellia cipher algorithms

項目名の左隣に<M> マークがつけば有効となります。

$ make
$ make modules_install
$ make install
以上で、インストールが完了です。reboot し、インストールしたカーネルバージョンで起動してください。

(4) Camellia 対応済み OpenSSL ソースの取得
http://www.openssl.org/source/から openssl-0.9.8c.tar.gz をダウンロードします。

(5) OpenSSL のコンパイルとインストール
$ tar xvfz openssl-0.9.8c.tar.gz
$ cd 展開したディレクトリ
$./config enable-camellia shared
$ make depend
$ make
$ make install
以上で、/usr/local/ssl 配下に OpenSSL がインストールされます。

(6) ipsec-tools ソースと『ipsec-tools CVS HEAD 20061002 への Camellia 追加パッチ』の取得
ipsec-tools ソースを CVS HEAD からチェックアウトしてください。
$ cvs –d anoncvs@anoncvs.netbsd.org:/cvsroot co ipsec-tools
同じディレクトリに、『ipsec-tools CVS HEAD 20061002 への Camellia 追加パッチ』を Camellia HP からダウンロードします。ダウンロードしたファイルを camellia-ipsec-tools-cvs-20061002.patch.gz とします。

(7) ipsec-tools ソースへのパッチ
$ cd ipsec-tools
$ zcat ../camellia-ipsec-tools-cvs-20061002.patch.gz | patch -p0

(8) ipsec-tools のコンパイルとインストール
$ ./bootstrap
$ ./configure --with-openssl=/usr/local/ssl
$ make

$ make install

以上で、ipsec-tools のインストールは完了です。

usr/local/bin/setkey、 /usr/local/sbin/racoon のパスを忘れないように設定して下さい。

(9) IPsec の通信

racoon.conf の proposal と sainfo に “camellia” を追記して下さい。その他の IPsec に関する設定の詳細はマニュアルなどをご参照下さい。