広域回線データ暗号化に関する一検討

7Ｆ－4

北市　隆一，斎藤　譲，舟辺　千江子，岡崎　直宣，妹尾　尚一郎，厚井　裕司
三菱電機（株）情報技術総合研究所

１．はじめに

Ｎ－ＩＳＤＮやフレームリレー等の公衆網／広域網を介したＬＡＮ間接続やクライアント／サーバ通信が一般化されていくにつれて，公衆網／広域網上でのデータの盗聴，公衆網／広域網を介してネットワークへの不正侵入といった脅威が増加してきた．ネットワークセキュリティを確保する対策は様々考えられている[1]．本稿では，ネットワークセキュリティ対策として公衆網／広域網上で送受信されるデータの暗号化について検討する．

２．広域回線上の送受信データの暗号化で確保されるセキュリティ

広域回線上の送受信データを暗号化することで以下のセキュリティが確保できる．

① 広域回線上のデータは暗号化されているので，広域回線上で盗聴は不可能である．

② 例えば，あるネットワークに広域回線から侵入しようとしたとき，たとえそのネットワークにアクセスするための回線番号等が判明してしまい，侵入者が回線を接続できたとしても，暗号装置は侵入者からのデータを復号してしまうので，侵入者のデータはただの数列と化してしまい，侵入も不可能となる．

３．広域回線上の送受信データ暗号化

広域回線上を送受信されるデータを暗号化する方法は，大きく分けて３通り考えられる．

①ＷＡＮプロトコル処理で暗号化する．

②ＬＡＮプロトコル処理で暗号化する．

③クライアント／サーバ間で使用するアプリケーションで暗号化する．

広域回線上での暗号化は回線上のデータすべてを暗号化することが前提とされるので，③については検討しない．上記①，②を用いたネットワーク構成例を図１に示す．また①，②の特徴について比較した結果を表１に示す．表１より，広域回線上での暗号化はやはりＷＡＮプロトコル処理で行うほうが，有利だと判断できる．

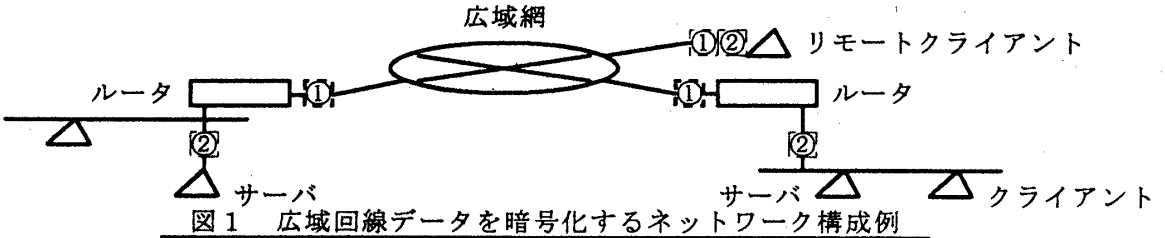

図１　広域回線データを暗号化するネットワーク構成例

A Study on Encryption of LAN Data on WANs

Ryuichi KITAICHI, Yuzuru SAITO, Chieko FUNABE, Naonobu OKAZAKI, Shoichiro SENO, Yuuji KOUI
Information Technology R&D Center, Mitsubishi Electric Corporation,
5-1-1 Ofuna, Kamakura, 247 Japan

表１　暗号化を行う処理部別特徴

	長所	短所
①	・一つのＷＡＮプロトコル処理上でＬＡＮプロトコルを選ばず，暗号がかけられる． ・例えばルータに実装した場合，複数の広域回線で，暗号をかける／かけないの設定が容易	・対象とする広域回線でしか，暗号がかからない．
②	・広域回線に限らず，暗号化が可能．	・ＬＡＮプロトコルごとに暗号処理を持つ必要がある． ・暗号をかける広域回線が経路となっているすべての宛先に対して暗号の設定をする必要がある．

４．広域回線暗合時の暗号化鍵変更

本稿では，暗号鍵変更処理の簡便化を図るため，暗号通信を行っている相手装置と１対１で暗号化鍵変更の動作を行う方法を検討する．広域回線暗合時の暗号化鍵変更タイミングを以下に示す．

ａ）日時や時間間隔を用いて一定間隔で鍵を変更する．

ｂ）広域回線接続時に鍵を変更（設定）する．

確実に鍵変更を行うために，鍵変更中はユーザデータの送受は行わなず，その間に受信したデータは廃棄することを前提とし，上記２つの方法について表２に比較結果を示す．

表２　暗号化鍵変更タイミング別特徴

	長所	短所
ａ）	・ユーザデータの少ないタイミングを選んで鍵変更できる ・鍵変更のタイミングを変えることで任意にセキュリティ強度を選択できる	・ユーザデータがない場合でも，設定時刻になると，回線を接続する必要がある． ・鍵変更のために回線を接続しようとして，回線が接続できない場合，鍵変更が行えないことがありうる
ｂ）	・回線接続時なので，ユーザデータの量も少なく，廃棄が少ない ・鍵変更のために回線を接続する必要がない	・使用する広域回線が専用線やＰＶＣの場合，鍵変更が装置立ち上がり時しか行えない

表２より，ＩＳＤＮなどで回線交換を用いるときはｂ）を，専用線やＰＶＣ接続の時はａ）と接続する広域回線によって鍵変更タイミングを変えるべきだと判断する．

５．最後に

本稿では，広域回線上のデータの暗号化について検討し，その暗号処理部，暗号化鍵変更タイミングを決定した．今後は，実際に広域回線暗号装置を本稿での検討内容を取り入れて作成し，実用上の評価を行うことが課題である．

参考文献：[1]William R.Cheswick, Steven M.Bellovin:Firewalls and Internet Security(1994)