広域網における暗号鍵の共有方法の検討

7F－3　斎藤　譲，北市　隆一，舟辺　千江子，岡崎　直宣，妹尾　尚一朗，厚井　裕司
三菱電機（株）情報技術総合研究所

１．はじめに

ＩＳＤＮやフレームリレー（ＦＲ），ＡＴＭ，専用線などの広域網（ＷＡＮ）を利用したクライアント／サーバシステムやＬＡＮ間接続が普及するにつれ，広域網上でユーザデータが盗聴されるという脅威も増えてきた．データ盗聴の対策の一つとして，データの暗号化を行うことが考えられるが，広域回線上のデータを暗号化する為には，広域網に直接接続するネットワーク構成機器において，暗号化／復号処理に用いる鍵の共有が必要となる．本報告では，広域網を介した鍵の共有方法の実現例を提案し，それらについて比較検討を行った．図１にＩＳＤＮを利用したＬＡＮ間接続及びクライアント／サーバシステムにおけるＷＡＮ上データの暗号処理の概念を示す．

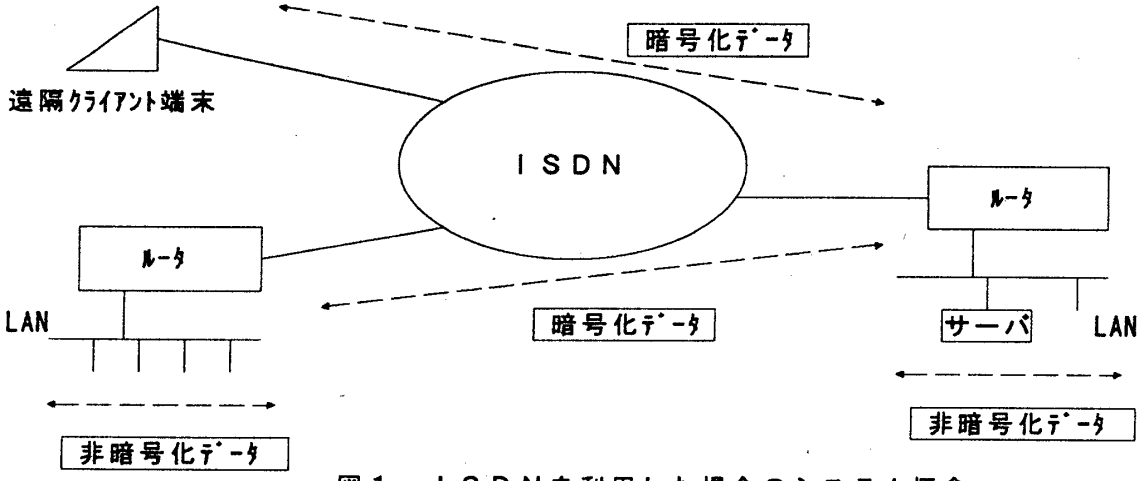

図１　ＩＳＤＮを利用した場合のシステム概念

２．暗号鍵の共有方法

上記のようなネットワークシステムにおいて，ＷＡＮに接続するネットワーク構成機器が暗号鍵を共有する実現例を以下に示す．

（１）ユーザ手設定による共有
各ネットワーク構成機器に対し，ユーザが入力した暗号鍵もしくは鍵に関する情報を元に暗号鍵を生成し鍵を共有する．

（２）時刻情報を用いた共有
各装置に内蔵している時刻情報（時計）を元に暗号鍵を自動的に生成し鍵を共有する．

（３）ＷＡＮ上のデータ転送プロトコルを用いた鍵情報交換による共有
ＷＡＮ上の中継データ転送プロトコル（Ｘ．２５［1］，ＰＰＰ［2］，ＦＲ［3］）において，暗号鍵に関する情報を交換する独自の手順を実装して共有する．

（４）ＩＰ上のアプリケーションを利用した鍵情報交換による共有
例えばＩＰ上のＵＤＰ手順を利用して暗号鍵に関する情報を各ネットワーク構成機器において交換し共有する．

（５）鍵管理装置からの配布による共有
ＷＡＮ上の鍵情報を管理する鍵管理装置により各ネットワーク構成機器に鍵情報を配布する．

Key sharing over wide area networks
Yuzuru Saito, Ryuichi Kitaichi, Chieko Funabe, Naonobu Okazaki, Shoichiro Seno, Yuji Koui
Information Technorogy R&D Center, Mitsubishi Electoric Corporation
5-1-1 Ofuna, Kamakura, Kanagawa, 247, Japan

3．実現例の比較検討

表１に各実現例に対する比較検討結果を示す．

表１　比較検討結果

番号	実現例	利点	欠点
（１）	ユーザ手設定による共有	・ｲﾝﾌﾟﾘﾒﾝﾄが容易	・人間が介在する為ｾｷｭﾘﾃｨ強度が低い ・利便性が低い(保守負荷が高い)
（２）	時刻情報を用いた共有	・各装置に共通の時刻情報を用いる為，鍵情報の交換が不必要であり，ｲﾝﾌﾟﾘﾒﾝﾄが容易	・時刻情報の誤差により，鍵の不一致が発生する． ・時刻情報より鍵を生成するのでｾｷｭﾘﾃｨ強度が低い
（３）	ＷＡＮ上のデータ転送プロトコルを用いた鍵情報交換	・鍵情報の交換を行うので，鍵の共有が確実に行われる． ・ﾕｰｻﾞｰの手を煩わせずに，鍵の生成ができ利便性が高い ・鍵情報と通信パスの対応付けが容易	・WAN上に鍵関連情報を転送するので，鍵情報の盗聴に対して，配慮が必要 ・ｲﾝﾌﾟﾘﾒﾝﾄが上記案と比較してやや難易度が高い ・課金される．
（４）	ＴＣＰ／ＩＰ上のアプリケーションを利用した鍵情報交換	・鍵情報の交換を行うので，鍵の共有が確実に行われる． ・ﾕｰｻﾞｰの手を煩わせずに，鍵を生成ができ利便性が高い ・WANに直接接続していない装置間や，複数の異なるﾈｯﾄﾜｰｸを介した装置間でも実現可能であり拡張性が高い	・ｲﾝﾌﾟﾘﾒﾝﾄが上記案と比較して難易度が高い ・課金される． ・鍵情報と通信パスの対応付けが難しい
（５）	鍵管理装置からの配布による共有	・鍵情報を鍵管理装置で一括管理できるので保守性がよい	・鍵管理用の装置を各ネットワーク毎に設ける必要がある． ・課金される． ・鍵情報と通信パスの対応付けが難しい

上記にあるように，ＷＡＮ上のデータを暗号化するだけならば，ＷＡＮ上のデータ転送プロトコルを用いて鍵情報を交換する方法が適当と思われる．ただし，暗号化範囲を単一のＷＡＮだけに限らず，暗号機能を有さない中継機器を介した通信パスや，ＷＡＮ／ＬＡＮを含めた通信パス上のデータを暗号化するような拡張性を考慮すると，ＩＰ上のアプリケーションを利用した鍵交換による共有方法が望ましい．また一括管理ができるという点においては鍵交換管理装置から配布する方法も有効である為，鍵管理装置においてＩＰ上のアプリケーションを作成し，配布するという（４）と（５）を組み合わせた方法が最適と考えられる。

4．まとめ

ＷＡＮ上のデータを暗号化する為に，ＷＡＮに接続するネットワーク構成機器間で暗号に必要な鍵の共有方法の比較検討を行った．今後は，鍵管理装置からの配送や、鍵情報の交換を行うアプリケーションのフィージビリティについてさらに調査し，ＷＡＮ上に限らず大規模なネットワークシステムにおける鍵の共有方法を検討する予定である．

＜参考文献＞
1：ＩＴＵＴ－Ｘ．２５
2：ＲＦＣ１６６１　The Point to Point Protocol
3：ＩＴＵＴ－Ｑ．９２２