7F－2

ネットワークセキュリティ（盗聴防止）とセキュリティドメインに関する一考察

馬場　義昌，妹尾　尚一郎，渡辺　晃，厚井　裕司
三菱電機（株）情報技術総合研究所

１．はじめに

インターネットに代表されるコンピュータネットワークの広がりとともに，コンピュータシステムのセキュリティに関する様々な研究が行われている．特に，CERT[1]の警告によりLAN上での盗聴の危険性が指摘され，ネットワークセキュリティ[2]，特に盗聴防止技術の確立が求められている．著者らは，盗聴防止技術としての暗号技術に注目し，ネットワーク上でのデータの暗号化，およびセキュリティドメイン[3]の構築について考察を行った．

２．暗号技術とセキュリティドメイン

ネットワーク上の任意のエリアを，一つのドメインと考える．セキュリティドメインは，セキュリティ管理者によって統一したセキュリティポリシーにより守られているエリアである．図１に示すように，セキュリティドメインは，一つの端末から構成される場合もあるし，複数のネットワークから構成される場合もある．本稿では，同一のセキュリティポリシーにより守られている，分散したセキュリティドメインを，暗号技術を用いて相互接続する方式について比較検討を行った．具体的には，各セキュリティドメインの端点のネットワーク機器（Edgeデバイス）に暗号機能を搭載し，セキュリティポリシーの異なるエリア上での盗聴を防止する．

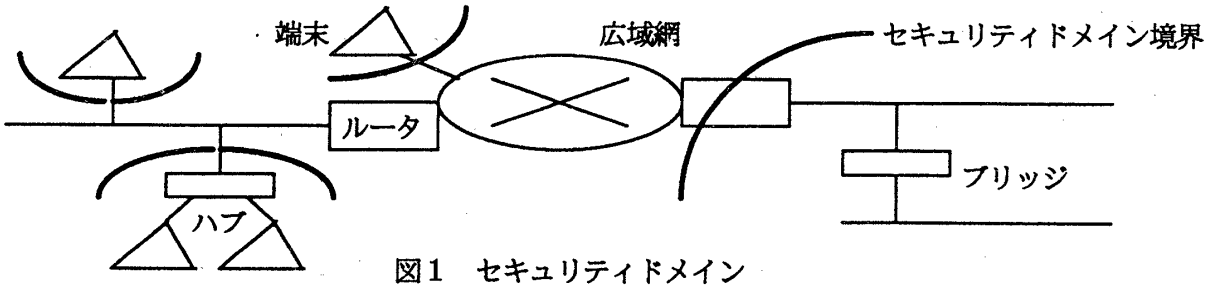

図１　セキュリティドメイン

３．セキュリティドメインの接続方法

同一のセキュリティポリシーにより守られている分散したセキュリティドメインを論理的に接続するには，次の方法が考えられる．

①各セキュリティドメイン間をメッシュ状に接続するPoint-To-Pointの仮想的な通信路（たとえばIPトンネル）を設け，その通信路上でエンカプセル化したデータを暗号化する．

②各セキュリティドメインのEdgeデバイスをセキュリティクライアントとして位置付け，セキュリティサーバとの間に仮想的な暗号通信路を設ける．セキュリティドメイン間の通信は，すべてセキュリティサーバを介した暗号通信路上で行う．暗号化方法は上記と同様．

③ユーザデータのトランスポート層以上を暗号化することにより，あたかも平文ネットワーク上に仮想的な暗号ネットワークを構築したかのように見せる．

A Study on Network Security and Security Domain
Yoshimasa BABA, Shoichiro SENO, Akira WATANABE, and Yuuji KOUI
Information Technology R&D Center, Mitsubishi Electric Corporation, 5-1-1 Ofuna, Kamakura, 247 Japan

上記の３方法についての比較結果を表１に示す．その結果，大規模なネットワークでは，セキュリティサーバを分散配置することにより性能等の問題に対処し，セキュリティ管理者が一つの暗号通信路を設定すればよい②の方法について必要とされる機能の検討を行った．

表１　セキュリティドメインの接続方法比較結果

接続方法	長所	短所
①	暗号通信路単位に暗号機能を選択可能	多数の暗号通信路を設定する必要があり，また使用する通信路を選択する処理が必要
②	一つの暗号通信路を設定すればよい	セキュリティサーバの性能が要求される 非効率的な経路になる場合がある
③	暗号通信路の設定を行う必要がない	プロトコル対応に仮想的な暗号ネットワークが必要

４．セキュリティサーバの機能

図２に，セキュリティサーバを分散配置してセキュリティドメインを相互接続する例を示す．セキュリティサーバは，各セキュリティドメインのEdgeデバイス（たとえば，端末のネットワークインタフェースカード(NIC)やハブ，ブリッジ，ルータ等）との間で，暗号通信路を設ける．また，セキュリティサーバ間にも同様な暗号通信路を設けることにより，セキュリティドメイン間の通信をすべて盗聴不可とする．セキュリティサーバに必要な機能を以下に示す．

・認証機能　Edgeデバイスからの接続要求に対して許可するかどうかを判断する機能．
・ルーティング機能　受信した暗号データを復号し，次の宛先へ暗号化してルーティングする機能．
・トンネリング機能　暗号通信路の確立と，そこで使用される暗号関連パラメータの折衝機能

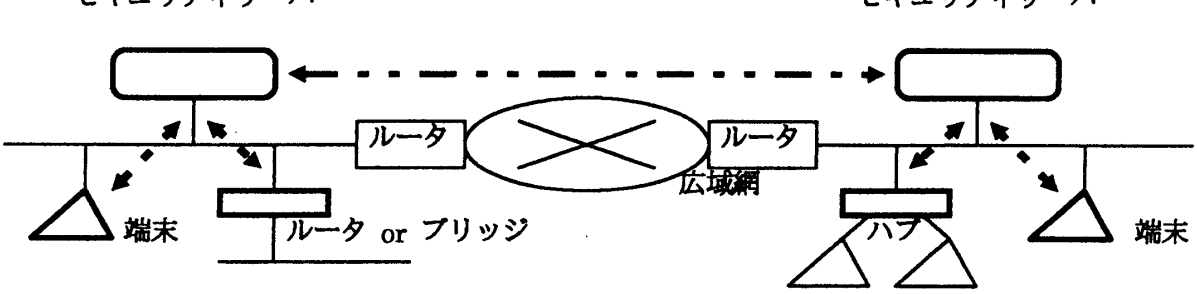

図２　セキュリティサーバの分散配置

５．まとめ

分散されたセキュリティドメインを，暗号技術を用いて相互接続する方法について検討した．その結果，セキュリティサーバを介したクライアント／サーバ型の通信路上で暗号通信を行う方法を提案する．また，大規模なネットワークに対しては，セキュリティサーバを分散配置する方法を提案する．今後は，セキュリティクライアント（Edgeデバイス）側の機能について，検討を行う予定である．

参考文献

[1] CERT(Computer Emergency Response Team) Advisory CA:94:01

[2] Charlie Kaufman, Radia Perlman, Mike Speciner : Network Security (1995)

[3] William R.Cheswick, Steven M.Bellovin : Firewalls and Internet Security (1994)