

# 暗号技術を用いたセキュア通信グループの構築方式とその実現

渡 邊 晃<sup>†</sup> 厚 井 裕 司<sup>†</sup> 井手口 哲夫<sup>†</sup>  
横 山 幸 雄<sup>†</sup> 妹 尾 尚 一 郎<sup>†</sup>

インターネットの普及に伴い、ネットワーク経由の脅威が大きな問題となっている。これを防ぐ方法として、暗号技術を用いて不正侵入や盗聴からユーザを守るセキュア通信グループの構築がある。本論文では、セキュア通信グループを構築する一方式として、グループを構成するすべてのコミュニケーションエンティティに対し、同一暗号鍵を与えるエリア定義方式を提案する。エリア定義方式はグループの定義が容易であり、IPのサブネットワークに依存しない通信端末単位のグループ化が実現できる。既存のパス定義方式と併用することにより、外部通信端末との通信も可能である。本提案の実現性を確認するため、端末とLANの間に設置するネットワーク暗号装置（NEU）を試作した。提案方式を実現するための具体的な仕様を設定し、ハードウェア、ソフトウェアの構成およびNEUの動作フローを提示した。評価の結果、スループット、ディレイ時間とも、LAN上で十分実用となる性能を得ることができた。

## Realization Method of Secure Communication Groups Using Encryption and Its Implementation

AKIRA WATANABE,<sup>†</sup> YUJI KOJI,<sup>†</sup> TETSUO IDEGUCHI,<sup>†</sup>  
YUKIO YOKOYAMA<sup>†</sup> and SHOICHIRO SENO<sup>†</sup>

With the spread of the Internet, threats through networks, such as intrusion and eavesdropping, become a major problem. One way to protect users from such threats is establishment of Secure Networks using cipher technology. In this paper, we suggest "Area-based definition" to define secure communication groups in which all communication entities share the same encryption key. By this way, it is easy to define communication groups independent of IP sub-networks. Communications with outside networks are also possible by combined use of the existing "Pass-based definition". To verify usefulness of our suggestion, we have implemented Network Encryption Unit (NEU) which is set between a terminal and a LAN. Concrete specifications, hardware/software constructions and operational flows are specified and realized. The result of its evaluations shows that its performance such as throughput and delay time is high enough for practical use on LAN.

### 1. はじめに

通信形態の変遷に伴い、ネットワーク上でのセキュリティが大きな問題となっている。特にインターネットは多様な組織にわたるオープンなネットワークであり、データの安全性について誰も保証してくれない。インターネットを介して相互接続されたシステムは、今後ますます増加すると考えられ、不正侵入や盗聴からユーザを守る安全なネットワークの実現が重要な課題である。

ネットワークシステムにおけるセキュリティ技術を大きく分類すると、2つに分けられる。第1は、ネッ

トワークは危険なもののみなし、アプリケーション側でセキュリティを確保するアプリケーションセキュリティ技術、第2は、ネットワーク自体の安全性を確保しようとするネットワークセキュリティ技術である。

アプリケーションセキュリティ技術はEC (Electric Commerce) やCALS (Commerce At Light Speed) の分野で技術が確立しつつある<sup>1)</sup>。SSL (Secure Socket Layer)やS-HTTP (Secure Hypertext Transfer Protocol) 等、これらのアプリケーションセキュリティを実現しやすくするための枠組みが標準化されようとしている<sup>2),3)</sup>。これらの方式は、アプリケーションに応じたセキュリティ対策が可能であるが、アプリケーションごとに異業種間で新しい規則やルールの調整が必要である。

ネットワークセキュリティ技術の1つとして、特定

<sup>†</sup> 三菱電機株式会社情報技術総合研究所高速通信部  
Information Technology R&D Center, Mitsubishi Electric Corporation

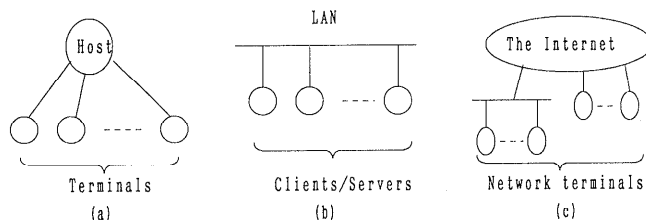


図 1 通信形態の移り変わり

Fig. 1 The change of communication style.

の装置間の通信パケットを暗号化することにより第三者による盗聴，侵入から保護された通信グループ（以下，セキュア通信グループと呼ぶ）を構築する技術がある。これは企業内通信，いわゆるイントラネットのインフラの構築に適しており，今後研究が盛んになると考えられる。これらの動きを支援する技術として，IP パケットの暗号化フォーマットや暗号鍵の共有方式等を規定している IPSEC が RFC 化されている<sup>4)~8)</sup>。しかし，IPSEC では通信グループの定義方法に関しては規定していない。

これまでの通信グループの定義方法として，コミュニケーションエンティティ間の通信パスをすべて個別に指定するパス定義方式がある<sup>9)</sup>。これは柔軟なシステム構築が可能であるが，規模が大きくなると設定が非常に複雑となる。そのためコミュニケーションエンティティを通常サブネット単位とし，暗号化エリアも広域網のみを対象とするのが一般的である。

本論文では，セキュア通信グループを定義するために，1つの暗号鍵を用いて通信グループを明示的に指定するエリア定義方式を提案する。エリア定義方式はグループの定義が容易であり，IP のサブネットワークに依存しない通信端末単位のグループ化が実現できる。さらにオープンシステムとのセキュア通信を可能とするため，パス定義方式を併用するハイブリッド方式を導入する。パケットの暗号化範囲については，既設のネットワーク機器に影響を与えないようにきめ細かく規定する。

提案方式の実現性を確認するため，通信端末と既存ネットワークの間に設置する LAN アダプタタイプのネットワーク暗号装置（NEU: Network Encryption Unit）を試作した。LAN 間対応の暗号装置はこれまでアイデアレベルの報告がある<sup>10),11)</sup>が，性能等についての詳しい報告は事例がない。

提案方式を実現するために必須となる仕様を設定し，高スループットを実現するためのハードウェア，ソフトウェアおよび処理フローを検討した。上記検討結果を試作装置に適用して性能を評価した結果，スループット，遅延時間とも 10BASE，TCP/IP 環境において十分実用となる性能を実現した。NEU の動作解析結果から，さらに高性能化を実現するための処理ネットワークを明らかにした。

本論文では以下，2章でセキュア通信グループの必要性と要件，3章で本提案方式におけるセキュア通信グループの実現方式，4章で試作と評価の結果について記述する。

## 2. セキュア通信グループの必要性と要件

### 2.1 必 要 性

ホストと端末をそれぞれ回線で接続し，個別に通信を実現するしかなかった時代は，通信経路が分離されていたため，ネットワークセキュリティが問題になることはほとんどなかった（図 1 (a) 参照）。1970 年代に複数の装置が伝送路を共有する LAN が出現した時，N:N 通信が実現可能となり，1980 年代半ば以降からクライアント/サーバシステムへとネットワークの再構築が図られるようになった（図 1 (b) 参照）。最新技術の活用や低コスト化の観点から，オープンシステムへの移行が決定的な流れとなり，CSMA/CD と TCP/IP が定着した。この頃より，ネットワーク経由の脅威が指摘されるようになった。

さらに WWW の登場が 1990 年代のインターネットの爆発的な発展へとつながり，世界中のネットワーク端末が相互接続されるのが現実となった（図 1 (c) 参照）。このようなネットワーク形態の変遷につれ，ネットワークセキュリティの状況は一変した。ネットワークに接続する無数のユーザには悪意を持つ者も含まれるため，盗聴や不正侵入が社会問題に発展することとなった。

インターネット技術を企業内ネットワークに適用するイントラネットにおいても，セキュリティに関する状況は同様である。企業内ネットワークは，第三者による不正侵入や盗聴から完全に守られている必要があり，ネットワークレベルで安全性を確保できるセキュア通信グループの実現は必須の課題である。

## 2.2 要件

イントラネットを実現するためのセキュア通信グループの要件を以下のように整理する。

- (1) 論理的なセキュア通信グループを容易に定義することができる。
- (2) IP のサブネットに依存しない通信端末単位のグループが構成できる。
- (3) セキュア通信グループと外部のオープンシステムとの間で通信を行うことができる。この場合でも外部とのセキュア通信が確保される。
- (4) ルータ等の既設のネットワーク機器や、アプリケーションプログラムに一切影響を与えない。

## 3. セキュア通信グループの構築方式

提案方式によるセキュア通信グループの構築方式を、既存の方式と比較しながら記述する。

### 3.1 既存技術による方法

既存技術によるセキュア通信グループの実現方法の例として、パス定義方式による場合を図2に示す。旧来からある1対1の回線暗号では、盗聴防止のみが目的であり、暗号鍵は通信ペアによりすべて異なるのが原則である。パス定義方式はこの考えの延長にある。図2において、CE<sub>i</sub>は通信端末またはそれらの集合を示すコミュニケーションエンティティ、MGEは暗号鍵を管理するマネジメントエンティティである。MGEはCE間の通信可否や暗号通信の有無を示す通信リストを保持する。この情報に従って、あらかじめ各CEに対し、通信可能な相手と暗号鍵を配送しておく（定期配送方式：図3参照）。MGEからCEへの鍵配送手順は通常の通信とは別に定義され、相互認証を含む確実な鍵配送を行う。

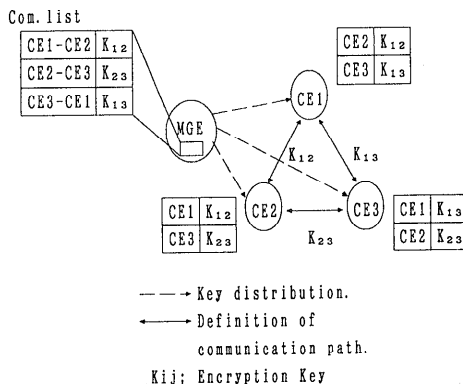


図2 パス定義方式によるセキュア通信グループの実現  
Fig. 2 Realization of a secure communication group using a path-based definition.

パス定義方式はすべての通信パスに対してパラメータを定義するため、平文通信との混在など、基本的にどのような通信形態も実現することができる。しかし暗号鍵を通信パスと同じ数だけ保持するため、規模が大きくなった場合鍵管理が繁雑となる。保持すべき暗号鍵の最大数  $N$  は、CEの増加に伴い急激に増加する。セキュア通信グループを構成するという観点から見ると、無駄が多い。

上記のような鍵管理の繁雑さを省く一方式として、通信要求が発生したタイミングで送受信CE間で鍵を共有する、随時配送方式がある（図4）。CE1とCE2が通信を開始する際、MGEとの間で通信リストのチェックが行われる。暗号通信であれば暗号鍵の発生を含む暗号鍵の共有手順が実行され、その後、一般の暗号通信が可能となる<sup>12)</sup>。

随時配送方式ではMGEでの繁雑な鍵管理から解放されるが、新たに以下の課題が発生する。すなわち、

- (1) 通信ペアの確立に先立つ鍵共有手順により、初期遅延が発生する。
  - (2) 鍵共有手順が走行したとき、すでに確立されていた別の通信ペアの通信を阻害する可能性がある。
- (2)を解決するためには、鍵共有手順を中継処理とは

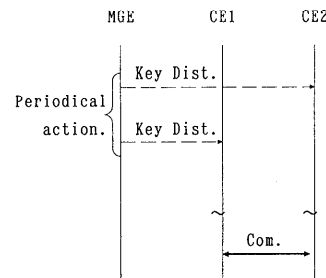


図3 定期配送方式による鍵共有  
Fig. 3 Key sharing by periodical distribution.

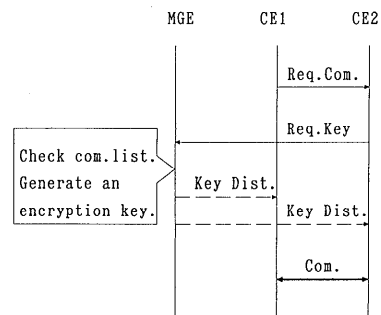


図4 随時配送方式による鍵共有  
Fig. 4 Key sharing on demand distribution.

別プロセサで実現する方法が考えられるが、コストが増加する。

### 3.2 エリア定義方式による実現方法

#### 3.2.1 エリア定義方式の概要

エリア定義方式は、セキュア通信グループを線の集合としてでなく面として明示的に定義し、これに唯一の暗号鍵を割り当てるものである。この考え方を基本にすることにより、後で述べるように暗号鍵の配送方法やオープンネットワークとの通信方法に対する考え方が変わる。

図5にエリア定義方式によるセキュア通信グループの実現方法を示す。セキュア通信グループを構成するすべてのCEに対し、同一の暗号鍵を与える。各CEは自分のセキュア通信グループを構成する暗号鍵“K”だけを保持する。Kを持たないCEはセキュア通信グループの通信内容を盗聴できないし、内部にアクセスすることもできない。

本方式では、MGEで保持する暗号鍵の数はセキュア通信グループの数に制限される。このため暗号鍵の管理が簡単になり、定期配送方式を採用することができる。鍵配送は一般通信のトラフィックが少ない時間帯等を実施すればよいため、一般通信のスループットの低下を招かない。

#### 3.2.2 鍵交換周期について

定期配送方式をとった場合、セキュリティ上鍵の交換周期が問題になる。ここでは盗聴等を除き、ネットワーク以外のシステムとしての管理は万全であることを前提とする。

伝送路上の暗号文のみを盗聴して暗号鍵を解読する全数探索法においては、暗号鍵長 80 ビットの場合、スーパーコンピュータで約 700 年かかるとされる<sup>13)</sup>。鍵長を十分長くすればこの時間は天文学的な数字とな

る。差分解読法および線形解読法では、いずれも大量の暗号文と平文のペアが必要である<sup>14)</sup>。したがって伝送路上の盗聴による脅威は無視できるといえる。

最も危険性が高いのは、物理的な盗難等により暗号鍵が外部に漏れる場合であり、これによりシステム全体が危険にさらされる。これに対しては、暗号鍵を暗号化/復号用ハードウェアの内部に閉じこめて外部から読めないようにする方法が考えられる。

上記のような対策がとられていれば、鍵更新周期は十分長くてもかまわないが、安全のためシステムの再構築や管理者の交代にともなって実施するのが適切と思われる。

### 3.3 オープンネットワークとの通信

一般にオープンシステム上の資源へのアクセスは不可欠な場合が多いが、エリア定義方式は、そのままではオープンネットワークとの通信ができない。本論文ではこれを可能とするため、セキュア通信グループ外との通信においてはパス定義方式を部分的に採用する。ここではこれを外部パス定義と呼ぶ。外部パス定義においては、暗号に代わるセキュア通信の代替手段として、フィルタリング機能を導入する。この機能により、アプリケーションの指定、セッション確立の方向性指定等の限定が行える。

設定方法としては、通信相手のアドレスごとにフィルタ条件を設定するケースと、上記設定されたアドレス以外について一括してフィルタ条件を設定するケースがある。これらの使用法を明らかにするため、外部パス定義の内容をCE1に着目して図6に示す。

#### (1) 特定の外部パス定義 (図6(a) 参照)

通信したい外部CE<sub>i</sub>が少数で、アドレスが分かっている場合、外部CEのアドレスに対してそれぞれ個別に平文通信である旨とフィルタ条

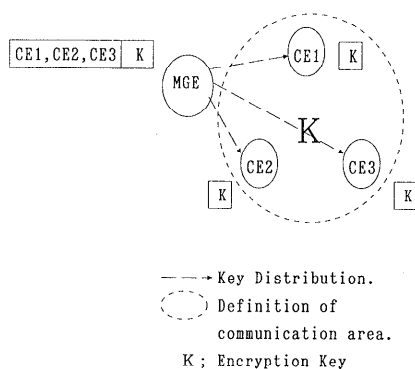


図5 エリア定義方式によるセキュア通信グループの実現  
Fig. 5 Realization of a secure communication group using an area-based definition.

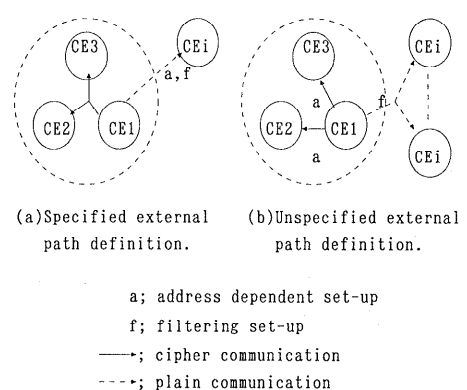


図6 外部経路定義の方法  
Fig. 6 Methods of external pass definitions.

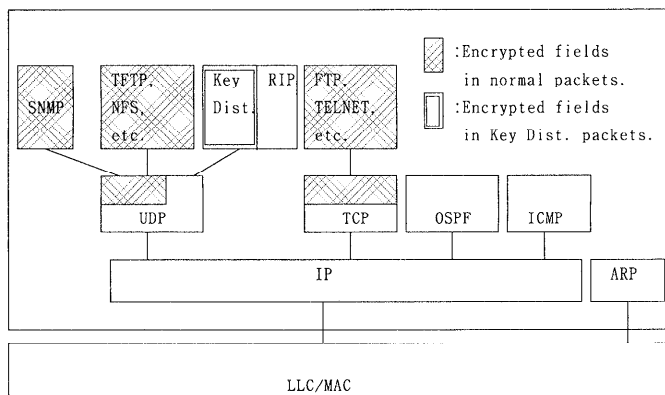


図7 TCP/IPプロトコル群と暗号化範囲

Fig. 7 The TCP/IP protocol suite and encryption fields.

件の設定を行う。上記アドレス以外に対しては、暗号通信である旨の設定を行う。大規模システムになると、通常外部端末へのアクセスにはプロキシサーバを介在する場合が多く、この方法が適している。

## (2) 不特定多数の外部パス定義 (図6(b) 参照)

外部CE<sub>i</sub>が不特定多数ですべてのアドレス指定が困難な場合、内部CEに対してそれぞれ個別に暗号通信である旨を設定する。上記アドレス以外に対しては、平文通信である旨とフィルタ条件の設定を行う。グループ内の通信に対しての設定が増えるので、大規模システムには向かない。プロキシサーバが設置されない小規模システムに適用できる。

### 3.4 パケットの暗号化範囲

暗号化したパケットがインターネットやLAN内のルータを越えて相手端末に到達できるように、パケットの暗号化範囲を定義する必要がある。暗号化/復号機能は端末そのものが持つこともできるし、外部の外付け装置が持つこともできる。ここでは試作装置に採用した外付け装置の場合を考える。

図7にTCP/IPプロトコル群とその暗号化範囲を示す。斜線部が暗号化対象部分である。ARP (Address Resolution Protocol) パケットは、ルータがプロキシARPを実現するため、暗号化せずそのまま中継しなければならない。ICMPパケットは、エラーが発生したときにルータが新たにエラー通知のために発生したり、ルータに対するテスト用として使用されることがあるため、暗号化してはならない。RIP、OSPFはルータ間の経路制御に使用されるパケットなので、暗号化してはならない。

TCPやUDPなどのユーザ情報が含まれるパケッ

トは暗号化の対象である。フィルタ条件としてアプリケーションの指定や、セッション確立の方向性指示等を行うことを考慮し、TCP/UDPヘッダのポート番号やTCPヘッダのCODEの部分は暗号化範囲からはずす。すなわちTCP/UDPヘッダの後半部分以降を暗号化範囲とする。

このように暗号化範囲を規定することにより、既存システムに影響を与えないセキュア通信グループの実現が可能となる。本方式では暗号化前と後でパケット長は変わらないため、暗号化にかかわるフラグメントが発生せず、高スループットを実現できる。

暗号鍵はUDP上に独自に定義された鍵配送用パケットにより配送される。鍵配送用パケットは複数の暗号装置を中継する可能性があるため、暗号化の対象外でなければならない。鍵配送用パケットの鍵情報の部分は通常のパケットとは別の暗号方式、たとえば認証と暗号化を同時に実現できるRSA方式<sup>15)</sup>を採用する。

### 3.5 システム構成例

提案方式によるセキュア通信グループを実際のネットワークに適用した例を図8に示す。図中、CEは通信端末 (Com. terminals)、MGEは管理装置 (Management Equipment) として示されている。ルータにより区切られるサブネットとは独立した、通信端末単位のグループを構成することができる。運用管理装置はシステム内の任意の場所に1台設置する。

外部パス定義により、グループ内からインターネット上のWWWサーバ等への外部アクセスが可能である。フィルタリング設定により、外部からのログインは禁止できる。LAN1ではプロキシサーバが設置されており、外部アクセスはすべてこのサーバを経由する。従って3.3節で述べた特定の外部パス定義を適用できる。LAN2ではプロキシサーバがない小規模システム

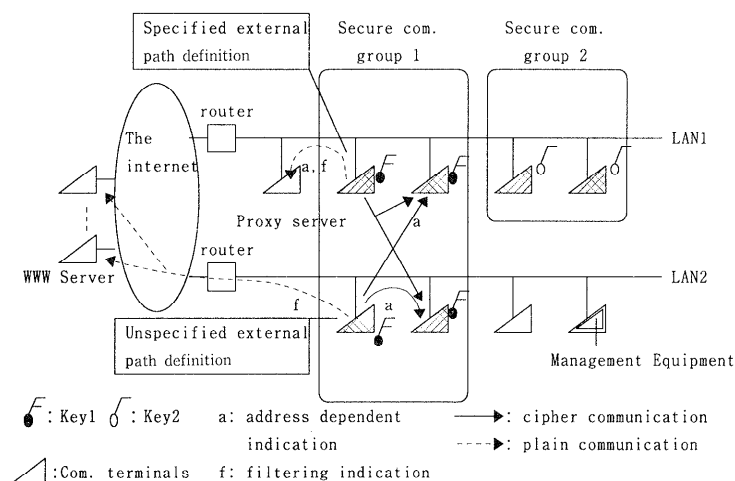


図8 セキュア通信グループの構成例

Fig. 8 A system example of secure communication groups.

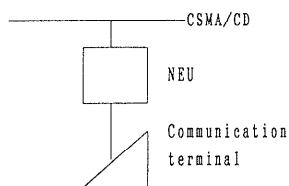


図9 NEUの実現位置

Fig. 9 A location of NEU.

の例で、不特定多数の外部パス定義を適用する。両者は共存してセキュア通信グループ1を構成することができる。

#### 4. 試作と評価

本提案のエリア定義方式によるセキュア通信ネットワークの実現性を確認するために、ネットワーク暗号装置を試作した。本章では提案方式を実現するために必須となる装置仕様、これを実現するための方式検討および試作装置の性能評価結果について記述する。

##### 4.1 仕様

###### 4.1.1 実現位置

通信端末単位のセキュア通信グループを構築するため、通信端末の外部に設置するLAN用アダプタを実現装置として選択した。試作装置はNEU (Network Encryption Unit) と称する。図9にNEUの実現位置を示す。アダプタ型は現実のネットワークに与える影響が少ないうえ、暗号鍵のセキュリティが守りやすいという利点がある。また独立した装置であることから、暗号鍵の配送方式として特定の方式を採用したり、他の暗号方式と併用することが可能である。このような外部設置型にした場合、コスト的に不利な面が出る

表1 NEUの仕様

Table 1 Specification of NEU.

| LAN インタフェース  | CSMA/CD                                         |
|--------------|-------------------------------------------------|
| 通信プロトコル      | TCP/IP                                          |
| データの暗号化/復号方式 | 独自方式                                            |
| 鍵配送/認証       | RSA                                             |
| セキュア通信グループ数  | 最大 32                                           |
| フィルタ設定数      | アドレス非依存: 1<br>アドレス依存: 64<br>(任意の上位有効レングス指定可)    |
| フィルタ条件       | TCP/UDP ポート番号 (それぞれ最大 8 ポートまで)<br>TCP コネクションの方向 |

が、これはNEUを暗号化機能を持つインテリジェント HUB として実現すれば回避することができる。

本機能を端末に内蔵する場合は、暗号鍵の漏洩を防ぐため、端末が立ち上がるたびに暗号鍵を配送する形態をとるのが望ましい。鍵配送時の認証識別子は、ユーザの身分証明書に入れておく等の検討を行う必要がある。

##### 4.1.2 仕様

表1に試作したNEUの仕様を示す。データの暗号化に用いる秘密鍵暗号方式は独自方式 (暗号鍵長 128 ビット)<sup>16)</sup>、鍵配送情報の暗号化には公開鍵暗号方式 RSA を採用した。セキュア通信グループの最大数は 32、アドレス依存型の設定条件の最大数は 64 である。

フィルタ条件として、TCP/UDP ヘッダのポート番号すなわちアプリケーションの指定をそれぞれ最大 8 個まで設定できる。TCP については CODE によりコネクション設定の方向を指定可能である。アドレス依存のフィルタ設定では複数アドレスの一括指定が可能のように、任意の上位アドレス有効レングスを指定

できる。

## 4.2 NEU の構成

### 4.2.1 ハードウェア構成

NEU のハードウェアブロック構成を図 10 に示す。LCN はネットワーク側の、LCT は端末側の CSMA/CD コントローラである。DRAM はプログラム実行エリアと、パケット送受信のバッファエリアを兼ねるメモリである。FLM は実行プログラムおよび設定パラメータ情報を保持するフラッシュメモリである。CPU はインストラクションキャッシュ 8K バイトを内蔵する、32 ビット RISC プロセサ（クロック速度：33 MHz）を採用した。ENC は DMA 機能と暗号化/復号用 LSI よりなる暗号処理部で、CPU から先頭メモリアドレスとレングスを指示すれば暗号化/復号処理を実施し、同一アドレス上に変換結果を残し終了割込みを通知する。

一方の CSMA/CD コントローラから受信したパケットは、暗号化/復号処理が施され、もう一方の CSMA/CD コントローラから送信される。この間パケットの DRAM 上でのアドレスは変わらない。すなわち CPU によるメモリムーブは行わない。これはスループットを確保する上で重要である。

LAN の 10 Mbps を滞留させることなく中継させるためには図 10 に示すように、DRAM 内のデータバッファへのアクセスが集中するため、少なくとも 10 Mbps の 4 倍の帯域が要求される。このとき、内部バス負荷  $F$  は式 (1) で表せる。

$$F = (\text{バスアクセス回数} \times k) \div \text{バスクロック}$$

$$= 10 \text{ Mbps} \times 4 \div 32 \text{ ビット} \times k \div 33 \text{ MHz}$$

$$(1)$$

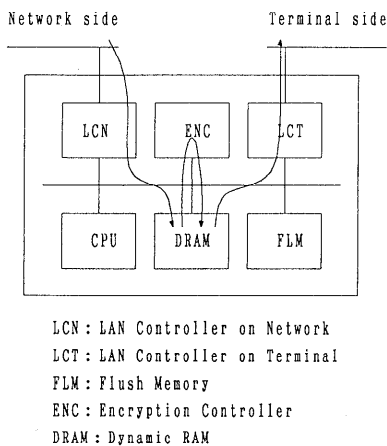


図 10 NEU のハードウェアブロック構成  
Fig. 10 Hardware structure of NEU.

ここで  $k$  は CSMA/CD コントローラまたは暗号処理部が DRAM1 ワードのアクセスに必要とするクロック数である。試作装置では平均 13 クロックを要しているため、これを適用すると式 (1) は  $F = 0.49$  となる。ここで中継処理において、CPU が DRAM アクセスを最小限に抑えることが必要である。これを実現するには、次に示すソフトウェア構成が前提となる。これにより図 10 のような単純な構成においても内部バス負荷が処理ネックにならないようにすることができる。

### 4.2.2 ソフトウェア構成

ソフトウェア構成は、筆者らが提案した中継装置特有の高速プログラミング技術を適用する<sup>17)</sup>。これによりハードウェアの性能を最大限に引き出し、中継性能のスループットを確保することができる。この方式の概要は以下のとおりで、中継処理にかかわるモニタのオーバーヘッドを減らすことと、CPU 内蔵のキャッシュヒット率を向上させるのがポイントである。

- (1) 一連の中継処理において、複数タスクに跨る処理でも制御をモニタに返さない。  
→ モニタオーバーヘッドの減少
- (2) 中継処理モジュールはメモリ上で連続的に配置させる。  
→ インストラクションキャッシュのヒット率向上
- (3) CPU の外部アクセスをできるだけ減らすテーパー構造。  
→ データキャッシュのヒット率向上
- (4) 他タスクに影響を与えないインタフェースモジュールの作成。  
→ 保守性の維持

(1), (2) により中継処理にかかわるインストラクションはすべてインストラクションキャッシュにヒットさせることができる。さらに (3) により外部データアクセスは 1 パケット処理あたり受信パケットのヘッダ部アクセス (8 ワード) に限定させることができる<sup>17)</sup>。

ソフトウェア全体のタスク構成とステップ数は、表 2 に示すとおりである。

## 4.3 NEU の処理

NEU の機能を実現する処理フローを図 11 に示す。受信パケットはまず自局宛か否かを判別し、自局宛であれば鍵配送等の管理処理を、それ以外のパケットは中継処理を行う。以下の中継処理を実現することにより、3 章で述べた提案内容をすべて満たすことができる。

- (1) 平文プロトコル識別  
アドレス解決プロトコル (ARP) やルータが使用するルーティング制御プロトコル (RIP 等) を識別し, 暗号化せずに中継する。
- (2) アドレス識別とフィルタリング処理  
アドレス識別後, 対応するアドレスの設定がある場合アドレス依存処理を, 対応するアドレスの設定がない場合アドレス非依存処理を実行す

表 2 タスク一覧とステップ数

Table 2 Role and program steps of tasks.

| モジュール     | 機能                                        | K ステップ           |
|-----------|-------------------------------------------|------------------|
| モニタ       | 割込み要因の識別, タスクのスケジューリング, タイマサービス, タスク間トレース | A: 1.0           |
| LAN ハンドラ  | LAN との送受信, エラー処理                          | A: 5.5<br>C: 1.6 |
| 暗号ハンドラ    | 受信パケットの識別, 精査処理, 暗号制御部に対する指示              | A: 0.8<br>C: 3.7 |
| コンソールハンドラ | パラメータの設定, 表示に対するオペレータインタフェース              | C: 8.1           |
| 装置管理      | プログラムロード, デバッグ, 自己診断                      | C: 14.3          |
| ネットワーク管理  | セッション鍵の復号, LSI への設定, 管理通信                 | C: 14.2          |

A: アセンブラ言語 C: C 言語  
ステップ数にコメント分は含まない。

る。設定内容に違反したパケットはフィルタリング処理で廃棄する。

### (3) 暗号化/復号処理

フィルタリング条件をクリアしたパケットに対し, 所定の暗号鍵でユーザデータ部分の暗号化/復号を行う。暗号化せず平文のまま中継する場合は, 暗号鍵をなしの設定にする。

## 4.4 評価結果

### 4.4.1 スループット

図 12 に最も単純なケースにおける試作 NEU のスループット測定結果を示す (アドレス非依存, フィルタ設定なし)。測定方法は, ルータのスループット測定に用いられるハーバードベンチマークテスト<sup>18)</sup>を採用し, 入力パケットと出力パケットの数を測定した。縦軸は伝送路負荷で正規化しており, 100% が CSMA/CD の理論限界である。

短パケット (64 バイト) においては, 9,430 PPS を実現し, 通常の CSMA/CD 対向ルータに匹敵するスループットが得られた。長パケット (1.5 K バイト) においては, 634 PPS, 伝送路負荷として 7.8 Mbps が得られた。

表 3 に設定条件の違いによる短パケット中継性能の測定値を示す。アドレス依存処理ではアドレス識別処理のため, 約 9% スループットが低下した。またフィルタ設定をした場合, フィルタなしの場合に比べ 5~6% スループットが低下した。

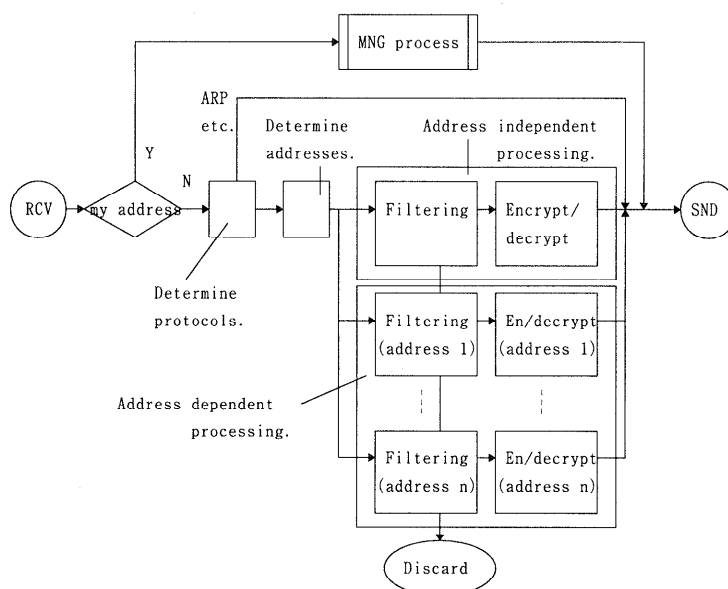


図 11 NEU の処理フロー

Fig. 11 Execution flow of NEU.

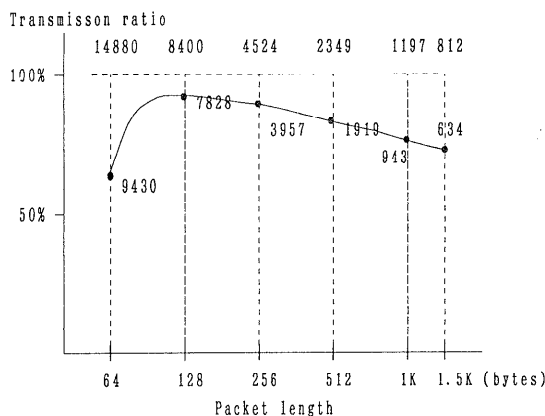


図12 NEUのスループット測定結果

Fig. 12 Measured value of total throughput in NEU.

表3 設定条件の違いとスループット

Table 3 Setting conditions and throughput.

| 設定条件    |             | スループット (PPS) |
|---------|-------------|--------------|
| アドレス非依存 | フィルタなし      | 9,430        |
|         | フィルタあり (1個) | 8,894        |
| アドレス依存  | フィルタなし      | 8,617        |
|         | フィルタあり (1個) | 8,198        |

#### 4.4.2 処理内容の解析

図13に図12と同様の条件下における中継処理の内訳を解析した結果を示す。単一の短パケットまたは長パケットを端末側から受信し、ネットワーク側に中継されるまでの処理において、LCT, LCN, ENC, CPUがそれぞれ走行した時間を示す。

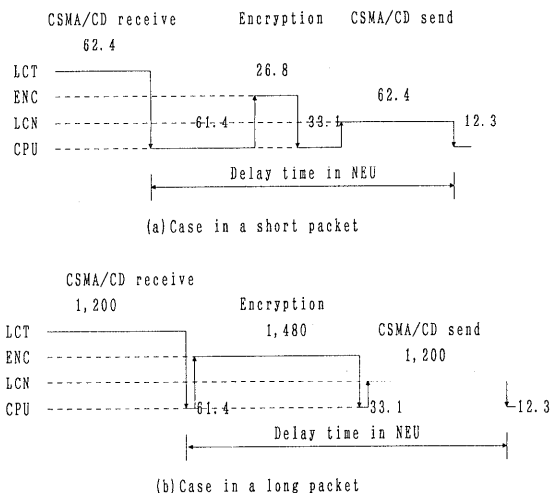
NEU内のディレイ時間は図13より、

- 短パケット … 184  $\mu$ s
- 長パケット … 2,775  $\mu$ s

となる。この値は、一般に市販されているルータが2段余分に入ったのと同程度と考えることができる。ルータを多段中継して動作できるアプリケーションから見れば、ほとんど問題となるディレイ値ではない。

#### 4.4.3 評価結果に対する考察

図13におけるCPU走行時間の合計の逆数をとると9,360PPSとなり、短パケットのスループット測定値とはほぼ一致する。このことより、短パケットにおける処理ネックはCPU処理であることが分かる。長パケットの場合、CPU処理時間は短パケットの場合と変わらない。一方、ENCの処理時間の逆数をとると680PPSとなり、長パケットのスループットとはほぼ一致する。すなわち長パケットにおいては、暗号化/復号のための変換時間が処理ネックであることが分かる。

図13 中継処理時間の内訳 (単位:  $\mu$ 秒)Fig. 13 Breakdown of processing time in relaying ( $\mu$ sec).

両者のネックがともに緩和される128バイト長において、最も高い伝送路負荷が得られている。

試作NEUにおいては、CSMA/CDコントローラ、暗号処理部、CPUのパイプライン動作がうまく機能したといえる。

CSMA/CDは衝突が多発するとレスポンスタイムが急激に増えることから、一般に伝送路負荷が30~40%以下になるようにシステム設計をする。測定結果から分かるように、NEUの性能はCSMA/CD上においては実用上ほとんど問題がない値が得られたといえる。NEUをさらに高速なLANに適用する場合、短パケットに対してはソフトウェア処理のさらなる高速化を、長パケットに対しては暗号LSIの高速化を考慮する必要がある。さらに、式(1)からも明らかのように、内部バス負荷が新たな処理ネックとなるため、高速メモリと高速バスアービタロジックの適用が必要になると考えられる。

## 5. む す び

同一暗号鍵を通信グループに与えることにより、セキュア通信グループを構築するエリア定義方式を提案した。外部との通信を可能とするため、外部経路定義とのハイブリッド定義方式を導入した。パケットの暗号化範囲を定義し、既存アプリケーションや既設ネットワーク機器に影響を与えないようにした。さらに提案方式を用いたシステム構成例を提示した。

提案方式の実現性を確認するため、ネットワーク暗号装置NEUを試作した。試作装置では、提案方式のシステム構築に必要な内容をすべて実現した。試

作装置を評価した結果、LAN 上の使用においてもほとんど問題のない性能を出せることが確認された。高速 LAN に適用するには、短パケットでは CPU の高速化、長パケットでは暗号 LSI の高速化が必須であることが分かった。

今後は本提案方式をさらに拡張し、エリアの重複、二重構成等に柔軟に対応できる定義方式等について検討を進める予定である。

### 参 考 文 献

- 1) バインズ：CALS/E・コマースのしくみ，技術評論社 (1996)。
- 2) Freier, A., Karlton, P. and Kocher, P.C.: SSL Version 3.0, Internet Draft, draft-freier-ssl-version3-00.txt (Dec. 1995)。
- 3) Rescorla, E. and Schiffman, A.: The Secure HyperText Transfer Protocol, Internet Draft, draft-ietf-wts-shhttp-01.txt (Mar. 1996)。
- 4) Atkinson, R.: Security Architecture for the Internet Protocol, RFC1825 (Aug. 1995)。
- 5) Atkinson, R.: IP Authentication Header, RFC1826 (Aug. 1995)。
- 6) Atkinson, R.: IP Encapsulating Security Payload (ESP), RFC1827 (Aug. 1995)。
- 7) Karn, P., et al.: The Photuris Session Key Management Protocol, Internet Draft, draft-ietf-ipsec-photuris-08.txt (Nov. 1995)。
- 8) Aziz, A., et al.: Simple Key-Management for Internet Protocol (SKIP), Internet Draft, draft-ietf-ipsec-skip-07.txt (Aug. 1996)。
- 9) 辻井, 笠原: 暗号と情報セキュリティ, 3.1, pp.57-59, 昭晃堂 (1990)。
- 10) Forne, J., Soriano, M., Melus, J.L. and Recacha, F.: Hardware Implementation of a Secure Bridge in Ethernet Environments, 0-7803-0917-0/93\$03.00c1993 IEEE (1993)。
- 11) 山口, 田中, 田辺, 小柳津: LAN の暗号通信における一方式, 信学技報, OFS93-32 (1994)。
- 12) 田中, 小柳津: UUI を利用した鍵配送方式の実装と評価, 信学論 (D-1), Vol.J78-D-1, No.6, pp.549-558 (1995)。
- 13) Schneier, B.: *Applied Cryptography*, Second Edition, John Wiley & Sons (1996)。
- 14) 今井: 暗号アルゴリズムの評価, 情報処理学会誌, Vol.37, No.6 (1996)。
- 15) Rivest, R., Shamir, A. and Adleman, L.: A Method for Obtaining Digital Signatures and Public-key Cryptosystems, *Comm. ACM*, Vol.21, No.2, pp.120-126 (1978)。
- 16) Matsui, M.: New Structure of Block Ciphers with Provable Security against Differential and Linear Cryptanalysis, *Third Interna-*

*tional Workshop of Fast Software Encryption*, Lecture Notes in Computer Science, Vol.1039, Springer-Verlag (1996)。

- 17) Watanabe, A., Kouji, Y., Seno, S. and Ideguchi, T.: Proposal and Performance Evaluation of a High-speed Internetworking Device, *IEICE Trans. Com.*, Vol.E79-B, No.5 (1996)。
- 18) Bradner, S.: Benchmarking Terminology for Network Interconnection Devices, RFC1242 (1991)。
- 19) 山口, 田中, 田辺, 小柳津: LAN 暗号通信方式の実装と評価, 信学技報, OFS93-38, pp.7-12 (1994)。
- 20) 渡邊, 平松, 藤井, 稲田: LAN における直列ブリッジ/ルータの検討, 信学技報, SSE94-41, pp.13-18 (1994)。

(平成 8 年 10 月 9 日受付)

(平成 9 年 1 月 10 日採録)



渡邊 晃 (正会員)

1974 年慶應大学電気工学科卒業。1976 年同大学院修士課程修了。同年三菱電機 (株) 入社。現在、同社情報技術総合研究所にて LAN, ネットワークセキュリティ等の研究開発に従事。電子情報通信学会会員。



厚井 裕司 (正会員)

1970 年東京理科大学理学部応用物理科卒業。同年、三菱電機 (株) 入社。以来、ネットワークアーキテクチャ, LAN, ネットワークセキュリティ等の研究開発に従事。現在、三菱電機 (株) 情報技術総合研究所勤務。電子情報通信学会会員。



井手口 哲夫 (正会員)

1972 年電気通信大学電気通信学部通信工学科卒業。同年三菱電機 (株) 入社。以来、ネットワークアーキテクチャ, LAN, ネットワーク管理方式, 通信プロトコル設計等の研究開発に従事。現在、三菱電機 (株) 情報技術総合研究所勤務。工学博士。電子情報通信学会会員。



横山 幸雄（正会員）

1983 年横浜国立大学工学部情報工学科卒業。1985 年同大学院修士課程修了。同年三菱電機（株）入社。現在、同社情報技術総合研究所にて、ネットワークセキュリティ、インターネット技術等の研究開発に従事。電子情報通信学会会員。



妹尾尚一郎（正会員）

1981 年東京工業大学理学部応用物理学科卒業。1983 年同大学院修士課程修了。同年三菱電機（株）入社。同社情報技術総合研究所にて、LAN、インターネット技術、ネットワークセキュリティ、電子メール等の研究開発に従事。

---