2T－5　暗号装置におけるアドレス検索ロジックの検討

稲田 徹　後沢 忍　時庭 康久　田口 卓哉　永島 規充　藤井 照子

三菱電機株式会社 情報技術総合研究所

１．はじめに

近年のインターネットを利用した通信の普及に伴い、セキュリティ対策として通信データ暗号装置が普及してきている。暗号装置には、ユーザのニーズに合わせたVPNを実現するためにIPアドレスとマスクを登録してセッション鍵を決定する機能が搭載されている。この機能は、通信データを受信した際、受信した通信データのIPアドレスと登録されたIPアドレスおよびマスクを比較し、条件にあった場合にその条件に対するセッション鍵を決定するものである。一般的にIPアドレスとマスクを使用して条件を登録する際、表１に示すようにある条件に他の条件が包含されるケースが発生する。このときの優先順位を決定する手法の一つとしてロンゲストマッチがある。ロンゲストマッチ処理の実現方法として、従来、ハッシュ関数を使用した方法が用いられてきたが、この方法の場合、テーブルの登録数によって処理時間がばらつくなどの問題があった。

本稿では、IPアドレスの１バイトごとにマスク値を反映したテーブルを用意し、高速にロンゲストマッチ処理を実現するテーブルジャンプ方式を提案し、その評価について記述する。

表１　IPアドレスとマスクを使用した条件例

条件	IPアドレス	ネットマスク	条件に含まれる端末ｱﾄﾞﾚｽ	処理
①	133.141.76.0	22ﾋﾞｯﾄ(0xFFFFFC00)	133.141.76.0～133.141.78.0	処理A
②	133.141.77.128	27ﾋﾞｯﾄ(0xFFFFFFE0)	133.141.77.128～133.141.77.159	処理B
③	133.141.77.142	32ﾋﾞｯﾄ(0xFFFFFFFF)	133.141.77.142	処理C

２．従来方式（ハッシュ方式）

ハッシュ方式では、IPアドレスでハッシュ値を計算し、ハッシュテーブルを生成し、ハッシュテーブルにネットマスクの長い順に条件テーブルをリンクする。表１に示した条件で生成されるテーブル構成を図１に示す。

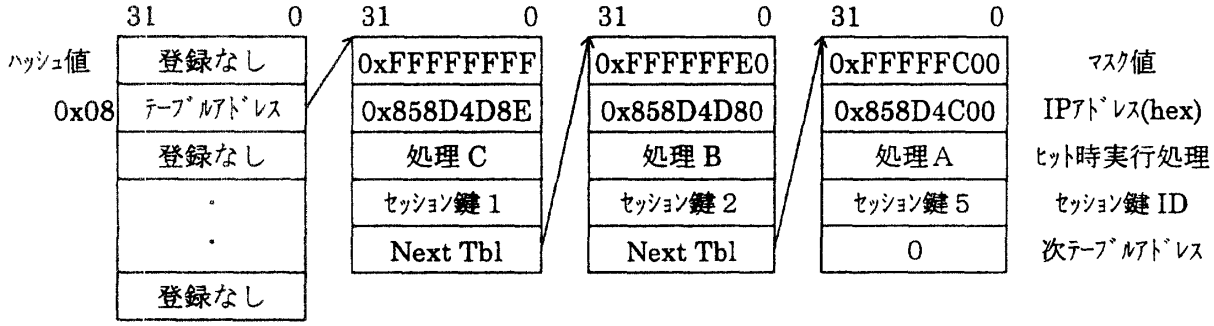


図１ハッシュテーブル構成

検索手順を以下に示す。

①受信フレームのIPアドレスからハッシュ値を計算

②ハッシュテーブルから最初にリンクされたテーブルを読み出し、受信フレームIPアドレスと登録されたマスク値のandをとる。

③②の値が登録されたIPアドレスと一致するかどうかチェックする。一致すれば、登録された処理を実行し、一致しなければ次テーブルアドレスを読み出し、②の処理を実施する。

以上のようにハッシュ方式の場合、リンクされるテーブル数が増加するにしたがって、処理速度が低下するという問題点がある。

３．テーブルジャンプ方式

テーブルジャンプ方式は、マスクを反映した形でのIPアドレス１バイトごとのテーブルを用意し、IPアドレスを直接オフセットとして実行処理を決定する方式である。表１に示した条件で用意されるテーブル構成を図２に示す。

A Study on Address Searching Method for an Encryption Unit

Toru INADA, Shinobu USHIROZAWA, Yasuhisa TOKINIWA, Takuya TAGUCHI, Norimitsu NAGASHIMA, and Teruko FUJII
Information Technology R&D Center, Mitsubishi Electric Corporation
5-1-1 Ofuna, Kamakura, Kanagawa, 247 Japan

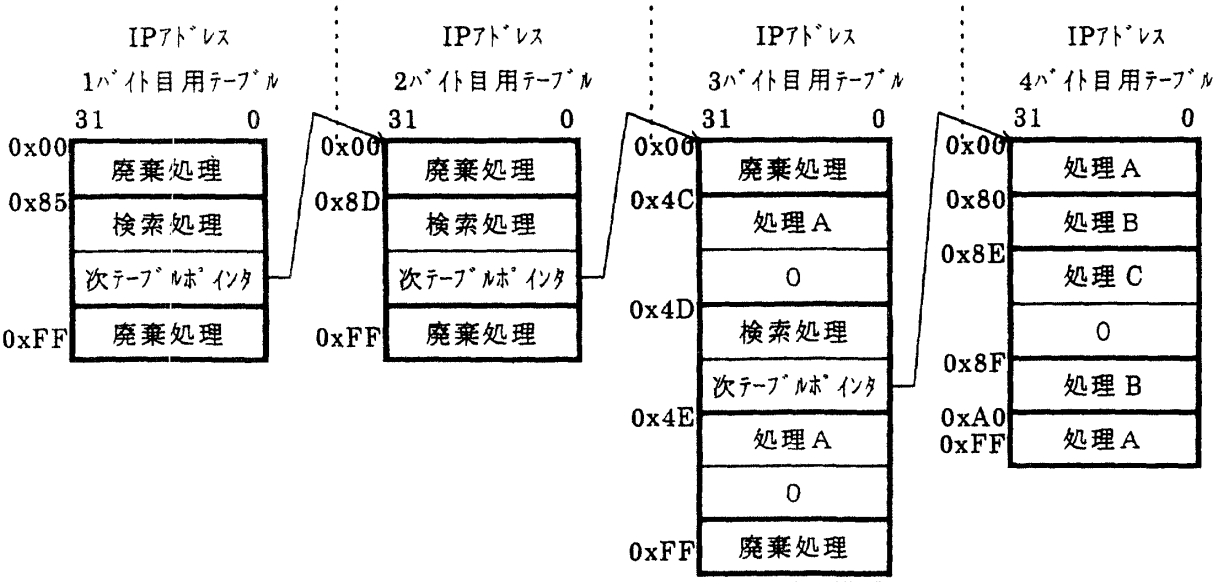


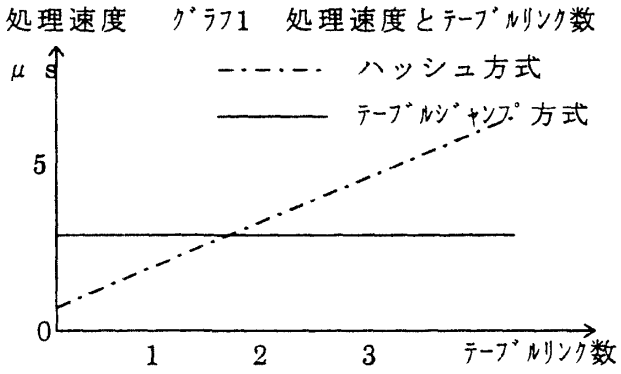
図２　テーブルジャンプ処理テーブル構成

検索手順は、IPアドレスのバイトをオフセットとしてテーブルを検索し、テーブルに設定されている処理を実行するのみである。このため、処理自体が小さくなり、さらにテーブルに次テーブルポインタ情報を設定し、処理を共通化することにより処理の占めるメモリ容量を削減することが可能となる。処理のメモリ容量の削減は、インストラクションキャッシュを使用した CPU を使用する場合に特に効果がある。

４．評価

４．１　条件数による比較

２章でも述べたようにハッシュ方式の場合、テーブルリンク数の増加によって処理速度が遅くなるという問題点がある。グラフ１にハッシュ方式とテーブルジャンプ方式のテーブルリンク数と処理速度の関係を示す。テーブルジャンプ方式がテーブルリンク数に依存しない検索処理方式であることがわかる。



４．２　暗号装置上での評価

テーブルジャンプ方式について、暗号装置上での評価を実施した。評価は、検索条件にヒットした場合、ヒットしない場合についてのスループットを測定することにより実施した（表２）。

表２　評価結果(単位 pps)

評価項目 / ヒットorミス	評価１	評価２	評価３	評価４	評価５
	条件なし	0～7ﾋﾞｯﾄﾏｽｸ	8～15ﾋﾞｯﾄﾏｽｸ	16~23ﾋﾞｯﾄﾏｽｸ	24~31ﾋﾞｯﾄﾏｽｸ
ヒットした場合	14352	14280	14284	14286	14205
ヒットしない場合		14308	14288	14288	14235

５．まとめ

ハッシュ方式に代わる IP アドレスの検索方式としてテーブルジャンプ方式を提案し、その評価を実施した。テーブルジャンプ方式は、ハッシュ方式と比較し、処理容量を小さく押さえることが可能で、特にインストラクションキャッシュ容量の制限される組込み型 CPU などに効果があり、また、実測値からも条件のマスク長、条件の数によらず、検索処理を実行しない場合とほぼ同等の処理速度を実現できることを確認した。

本方式は、IPアドレスのバイト毎にテーブルを用意する方式であるため、ハッシュ方式と比較し、メモリ使用量が大きくなるが、暗号装置のように条件設定数が比較的少ない装置については非常に有効である。ファイアウォールなど条件設定数が多い装置に適応するために、テーブルに登録する情報量を圧縮し、メモリ使用量を削減することが今後の課題となる。

参考文献

[1] 横山他：“LAN 用暗号装置の実現方式”，電子情報通信学会総合大会，1997