目　次

概　要

ネットワークにおけるセキュリティ上の脅威が問題となっており，通信パケットの暗号化技術が重要な技術として認識されている．既存の暗号化通信技術として IPsec ESP が挙げられるが，セキュリティは強靭なものの，NAT やファイアウォールを挟むような環境では使用できない，スループットが低下する，などの課題があり拠点間通信などの一部でしか利用されていない．そこで本論文では，NAT やファイアウォールと共存でき，かつオリジナルパケットのフォーマットを変えないまま本人性確認（正当な相手であることの保証）とパケットの完全性保証（パケットが改竄されていないことの保証）を実現する暗号通信方式 PCCOM（Practical Cipher COMmunication）を提案する．PCCOM の有効性を確認するために試作システムを FreeBSD 上に実装し，NAT やファイアウォールとの親和性が高いことを確認した．また，スループットを測定した結果，パケットフォーマットを変えないことによる性能上の効果があることを確認した．

1. はじめに

ネットワークにおけるセキュリティ上の脅威は年々深刻な問題となっており，セキュリティ技術の重要性が高まっている．その中でも，IPsec ESP（Encapsulation Security Payload）[1)~4)]のようにIP層でパケットの暗号化などを行うことによりネットワーク自体のセキュリティを確保するネットワークセキュリティ技術は，利用するアプリケーションを意識することなく安全を確保できることから，ネットワークの根本的なセキュリティ対策として期待されている．しかし実際にはIPsec ESPは，NAT/NAPT（Network Address Translator/Network Address Port Translator；以後NATと総称する）やファイアウォールを挟むような環境では使用することができず，普及が進んでいないのが現状である．このことから，ファイアウォールやNATとの共存が可能な暗号化通信は有効な技術と考えられる．しかし，セキュリティ強度と柔軟性・利便性といった実用度は相反する要素であり，ひとつの技術であらゆる要求に対応するのは困難である．従って今後のセキュリティ技術は，セキュリティ強度と実用度を想定する利用形態に応じて，それぞれに適した方式を検討することが重要になると考えられる．

IPsec ESPは，盗聴を防止する暗号化の他に，なりすましを防止する本人性確認（正当な相手であることの保証）や改竄を防止するパケットの完全性保証（パケットが改竄されていないことの保証）などの機能を提供している．また，ESPにはトランスポートモードとトンネルモードがあり，前者はEnd-to-EndのIPsec通信を適用する際に利用し，後者は主にGateway-to-GatewayやHost-to-GatewayのIPsec通信を適用する際に利用する．しかし現実の適用例を見ると，インターネットVPN（Virtual Private Network）の構築手段としてGateway-to-Gatewayでトンネルモードを用いる例を除くとあまり普及していない．これは，パケットの暗号化や完全性保証がもたらすNATやファイアウォールとの相性の悪さに起因している．これらの課題を解決するために，UDPヘッダで更にESPパケットをカプセル化してNATを通過させる方法（UDP Encapsulation of IPsec Packets）[5)]が提案されているが，カプセルヘッダの部分は完全性保証の範囲に含めることはできず，ヘッダの追加によるオーバヘッドの増加やフラグメントの発生などの課題が発生する．また，ESPの暗号化を階層化し，TCP/UDPヘッダの内容をルータやファイアウォールが参照できるようにするML-IPsec（Multi-Layer IPsec）[6)]が提案されているが，この方法では既存のシステムを変更する必要がある．

一方，7）ではパケットフォーマットを変えないまま特定の範囲を暗号化す

る方式が提案されている（以下，置換方式と呼ぶ）．置換方式は，ポート番号を平文のままとするため，ファイアウォールの通過が可能であり，パケットフォーマットを変えないためヘッダオーバヘッドやフラグメントが発生せず高スループットを実現できるという利点がある．しかし，置換方式では TCP/UDP チェックサム [8~10] を暗号化範囲に含めているため，NAT によるチェックサムの書き換えに対応できず，NAT を通過することができない．また単に平文と暗号文を置き換えるだけのため，本人性確認とパケットの完全性保証を実現していない．

本論文では置換方式の利点に着目し，置換方式を改良することによって，NAT とも共存でき，かつ本人性確認とパケットの完全性保証も確実に行える暗号通信方式 PCCOM（Practical Cipher COMmunication）を提案する．PCCOM は本人性確認とパケット全体の完全性保証を，共通秘密鍵とパケットの内容から生成した疑似データと呼ぶ値を用いて，TCP/UDP チェックサムを新たに再計算することにより実現する．この方法によると NAT やファイアウォールと共存することが可能で，かつパケットフォーマットを変えないためヘッダオーバヘッドやフラグメントが発生せず高スループットを実現できる．なお，PCCOM は事前に送信側と受信側で共通秘密鍵を共有していること，パケットの処理内容を記述した動作処理情報テーブルを既に保持していることを前提としている．

PCCOM の有効性を確認するために試作システムを開発した．PCCOM がパケットフォーマットを変えずに処理する方式であることが，実装の容易さをもたらし，性能的にも有利であることについて述べる．評価の結果，高スループットを実現できることを確認した．また，PCCOM の安全性評価を行い，IPsec ESP とのすみわけについて考察した．

本論文の構成は以下のとおりである．2 章で既存技術とその制約について説明した後，3 章で実用暗号通信 PCCOM を提案する．4 章では PCCOM の実装について説明し，5 章では実装したシステムを用いた PCCOM の性能評価を行い，PCCOM の安全性評価と，IPsec ESP とのすみわけについて述べる．最後に 6 章でまとめる．

2. 既存技術とその制約

IPsec ESP のトランスポートモードとトンネルモードのパケットフォーマットを図 1 に示す．

トランスポートモードでは，IP ヘッダとそのペイロードの間に ESP ヘッダを挿入し，元の IP パケットのペイロード部分を暗号化する．トンネルモードでは，

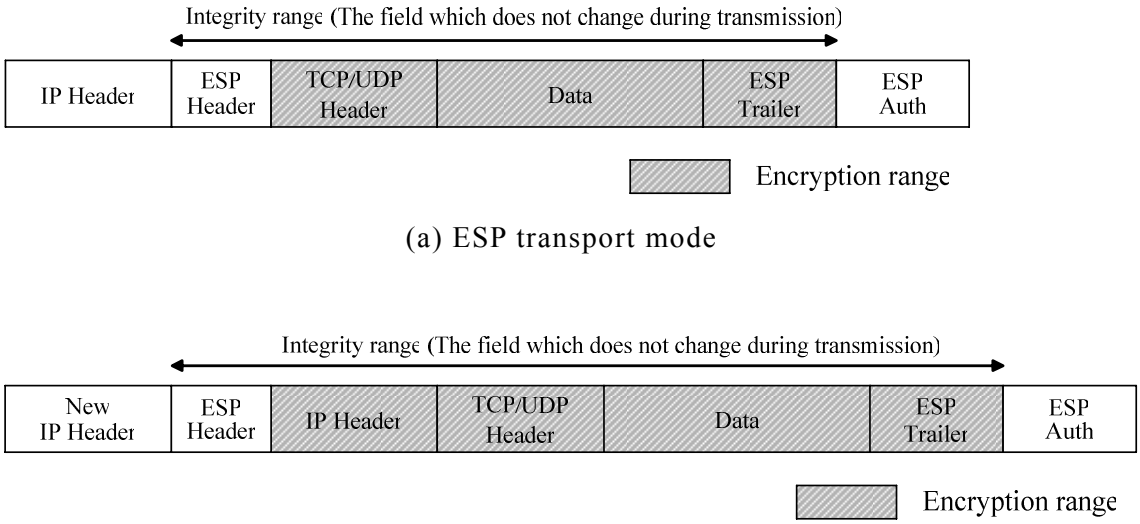


図 1　IPsec ESP のパケットフォーマット
Fig.1　Packet format of IPsec ESP.

セキュリティゲートウェイのアドレスを含む新しい IP ヘッダでカプセル化し，カプセル内のデータすなわち元の IP パケットを暗号化する．ESP トレーラは，ブロック暗号のブロック長の整数倍に暗号化するデータの長さを揃えるために用いる．また，ESP ヘッダから ESP トレーラまでの完全性を保証する認証値 ICV（Integrity Check Value）を計算し，ESP 認証値（ESP Auth）としてパケットの末尾に付加する．いずれのモードにおいても TCP/UDP のポート番号が暗号化範囲に含まれているため，そのパケットがどのような用途に用いられるかがファイアウォールで判別できない．その結果，ファイアウォールでは全ての IPsec の通過を禁止してしまう場合が多い．また，TCP/UDP チェックサムフィールドが暗号化範囲・完全性保証の範囲に含まれているため，IP アドレスの変換を伴う NAT を通過すると偽造パケットと見なされ，IPsec 処理によってパケットが廃棄される．これは TCP/IP が綺麗な階層構造になっておらず，TCP/UDP チェックサムでありながら IP アドレスもチェックサムの演算範囲に含んでいることが根本的な理由である．トンネルモードにおいては，IP アドレスのみを変換する純粋の NAT を通過することは可能であるが，ポート番号の変換も伴う NAPT（IP マスカレード）は通過できない．このような状況に対処するために，市販のルータにおいて，UDP

ポート500番のエントリを持っているノードに対してESPパケットを転送することでNATを通過させているものがある（IPsecパススルーと呼ぶ）が，この方法ではひとつのノードだけしか ESP の通信は機能しない．一方 IETF（Internet Engineering Task Force）では，UDPヘッダで更にESPをカプセル化してNATを通過させる方法（UDP Encapsulation of IPsec Packets）が提案されているが，カプセル部分は完全性保証の範囲に含むことはできず，ヘッダの追加によるオーバヘッドの増加やフラグメントの発生などの課題が発生する．

以上のことから，IPsec をシステムに導入するには既存設備との相性やスループットの低下を考慮する必要がある．

図 2 に，PCCOM のベースとなっている置換方式のパケットフォーマットを示す．暗号化後のパケットフォーマットはオリジナルフォーマットから変化させず，平文と暗号文をそのまま置き換える．ファイアウォールがポート番号を識別できるように，また TCP/UDP チェックサムから暗号文の内容が推測されるのを防ぐために，暗号化範囲を TCP/UDP ヘッダのチェックサムフィールド以降の全ての部分としている．TCP/UDP ポート番号が平文であるため，ファイアウォールによるフィルタリングが有効になるうえ，パケット長が変わらないためスループットの低下が少ないという利点がある．この方式はイントラネット内では有効であるが，TCP/UDP チェックサムフィールドが暗号化範囲に入っているためチェックサムの書き換えを伴う NAT を通過できない．また，本人性確認とパケットの完全性保証を実現していないため，なりすましや改竄の恐れがある．

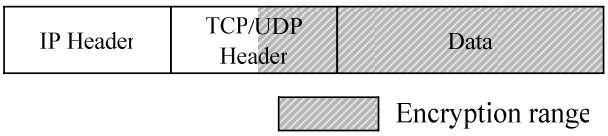


図 2　置換方式のパケットフォーマット
Fig.2　Packet format of the replacement method.

3. 実用暗号通信 PCCOM の提案

PCCOM が提供する機能は，暗号化による機密性確保，本人性確認とパケットの完全性保証である．また，NAT やファイアウォールとの共存ができ，パケット

フォーマットを変えないため高スループットを実現できるなどの特徴がある．なお，IP アドレスとポート番号は NAT で内容が変換されるため完全性保証の範囲に含めない．この部分の保証に関しては，パケットの処理内容を記述した動作処理テーブルの検索過程でその内容を保証する．

3.1. PCCOM の原理

PCCOM のパケットフォーマットを図 3 に示す．PCCOM では，共通秘密鍵とパケットの内容から生成した疑似データと呼ぶ値を用いて，TCP/UDP チェックサムに独自の計算を施すことにより，本人性確認とパケットの完全性保証を行う．以下にその原理を示す．

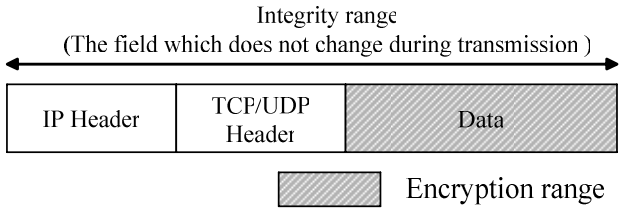


図 3　PCCOM のパケットフォーマット
Fig.3　Packet format of PCCOM.

PCCOM では本人性確認と完全性保証を実現するために，まず CB（Checksum Base）と呼ぶチェックサムベース値を定義する．CB は，IP ヘッダ，TCP/UDP ヘッダで転送中に値の変化しないフィールド（図 4 の灰色部分）と，事前に秘密裏に共有している共通秘密鍵を含めた値から生成したハッシュ値である．CB の種には共通秘密鍵の他にシーケンス番号のように初期値が乱数で決まりパケットごとに値が変化するフィールドを含んでおり，CB 値を第三者が推測するのは極めて困難である．この CB は，以下のように本人性確認とパケットの完全性保証を実現するためのキーデータとなる．

一般通信と PCCOM の，TCP/UDP チェックサムの計算範囲の違いを図 5 に示す．図中の点線はチェックサム計算時に疑似的に作成する情報を指す．一般の通信では TCP/UDP チェックサムは，TCP/UDP ヘッダ，TCP/UDP 疑似ヘッダ，ユーザデータから計算される．ここで，TCP/UDP 疑似ヘッダには IP アドレスの値を含む．このため，NAT を経由して IP アドレスが変わると，TCP/UDP チェックサムも書き換えが必要となる．一方，PCCOM では TCP/UDP チェックサムは，

IP Header

Version	IHL	Type Of Service	Total Length	
Identification			Flags	Fragment Offset
Time To Live		Protocol	Header Checksum	
Source Address				
Destination Address				

TCP Header

Source Port			Destination Port
Sequence Number			
Acknowledgement Number			
Data Offset	Reserved	Control Flag	Window
Checksum			Urgent Pointer

UDP Header

Source Port	Destination Port
Length	Checksum

The field to be used for generation of CB

図 4　CB 生成に用いるフィールド

Fig.4　The field to be used for generation of CB.

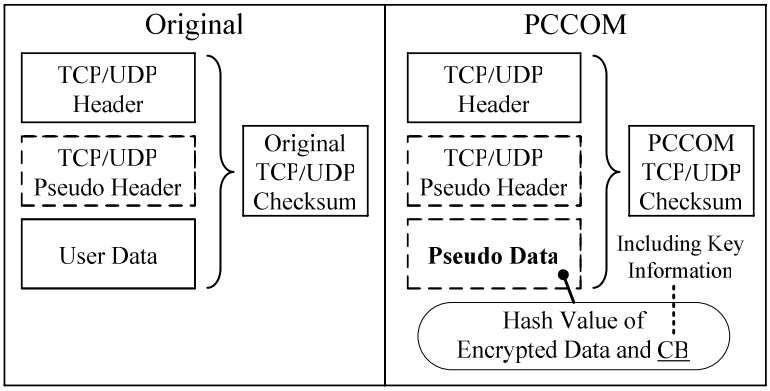


図 5　チェックサム計算範囲の違い

Fig.5　Calculation range of checksum.

TCP/UDP ヘッダ，TCP/UDP 疑似ヘッダ，疑似データから計算される．ここで，疑似データとは暗号化後のデータと CB を元に求めたハッシュ値である．

完全性保証の流れを以下に述べる．送信側ではデータの暗号化後，上記疑似データを用いて TCP/UDP チェックサムの再計算を行う．受信側ではデータの復号を行う前に，同様の方法で生成した疑似データを用いて TCP/UDP チェックサムを検証する．検証結果が正常であれば，復号を行いオリジナルチェックサムの再計算を行って上位層（TCP/UDP）に渡す．この方式により，暗号化データと CB 生成に用いたフィールドの完全性を保証することができると同時に，本人性確認も実現される．パケットの改竄者が改竄を隠蔽するために，パケットの一部を書き換えると同時に TCP/UDP チェックサムを再計算しようとしても，疑似データの内容が分からないので正しい計算を行うことはできない．なお，IP アドレスとポート番号は NAT にて変換されるので CB 生成の範囲には含めない．IP アドレスとポート番号の保証方法については次節で述べる．

上記の演算方式によると，通信経路上に NAT が介在して IP アドレス，ポート番号，チェックサムが書き換えられたとしても，完全性保証，本人性確認の考え方は維持される．なぜなら，NAT における TCP/UDP チェックサムの書き換えは，11）で規定されているように変換部分の差分を計算するだけであり，受信側で行うチェックサムの検証には影響を与えないためである．PCCOM ではパケットの暗号化範囲はユーザデータ部分のみとしているが，本人性確認とパケット全体の完全性保証が施されているため，パケットの偽造による TCP セッションハイジャックなどの攻撃を防ぐことができる．また，PCCOM ではファイアウォールが TCP/UDP ヘッダの内容を用いたフィルタリングを行うことが可能であるため，実用面でのメリットが大きいと考えられる．

暗号アルゴリズムとしては，任意長のデータを暗号化できるブロック暗号の CFB モードを採用する．よって，暗号化によってパケット長が変化することがなく，高スループットが実現でき，かつフラグメントの発生を懸念する必要がない．なお，暗号化で必要な初期値 IV（Initialization Vector）には CB 値を流用する．

3.2. IP アドレス・ポート番号の保証

PCCOM では，IP アドレスとポート番号は NAT を経由する際に値が変化するため CB 生成の範囲に含めていない．そのため，このままでは通信経路上で送信元アドレスの改竄や，ポート番号の改竄によるアプリケーションの誤作動などを招く可能性がある．これらを防ぐために，IP アドレスとポート番号の完全性は，パケットの処理内容を記述した動作処理情報テーブルの検索過程で保証する．テーブル検索の処理を図 6 に示す．動作処理情報テーブルとは IPsec における SAD（Security Association Database）に相当するもので，テーブル内には送信元と宛

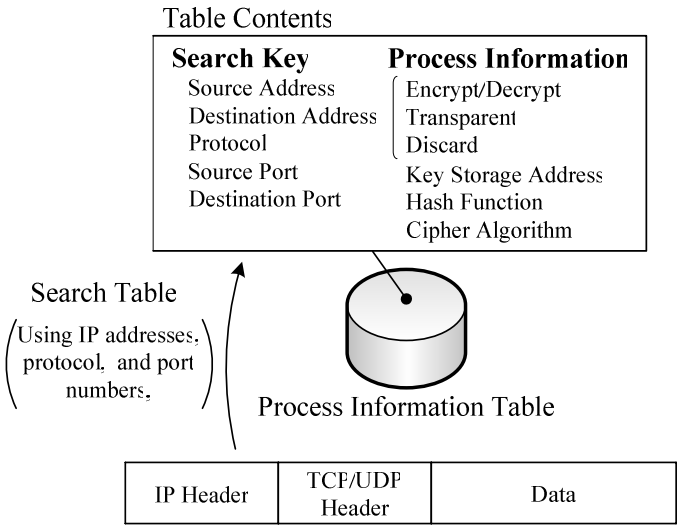


図 6　テーブル検索処理

Fig.6　Table search process.

先の IP アドレスとポート番号，プロトコル番号とそれに対応する，パケットの処理内容（暗号化/復号，透過中継，廃棄），使用する共通秘密鍵の格納場所，適用するハッシュ関数，暗号アルゴリズムが記述されている．送信側と受信側の両端末は通信の開始前に設定情報の交換を行い，両端末で，通信パケットの処理に必要となる動作処理情報テーブルを生成してカーネルに保存する．送信側の端末はパケット送信時に，受信側の端末はパケット受信時に，パケットの IP アドレス，ポート番号，プロトコル番号をキーに動作処理情報テーブルを検索し，その内容に従って暗号化/復号などの処理を実行する．従って受信側の動作処理情報テーブルを検索後，テーブルの内容から IP アドレス，ポート番号，プロトコル番号を再度確認し，テーブル内に該当パケットの情報が正しく存在したら，IP アドレスとポート番号は改竄されていなかったことが保証される．なお，一定時間以上参照されない動作処理情報テーブルのレコードは削除する．また，事前に設定した有効期限より長い間通信が継続された場合には，再度その内容を更新するための手続きが実行される．

この方式は事前に正しい内容のテーブルが生成されていることが前提となる．正しいテーブルの生成を保証する方式としては，IKE （Internet Key Exchange）[4)]などの既存の技術を流用することが可能である．ここで，IKE は安全な通信路を確立する SA（Security Association）と共通秘密鍵を管理するプロトコルであり，例えば，受信側での SA の特定には IP アドレス，ポート番号，プロトコル番号を用い，PCCOM 特有の部分を PCCOM DOI（Domain of Interpretation）として定義することにより，動作処理情報テーブルの生成が実現できる．

4. PCCOM の実装

PCCOM の試作システムを開発し，動作検証を行った．本章では試作システムの実装方式，仕様・構成と動作概要について記述する．

4.1. 実装方式

試作システムは，FreeBSD（5.3 Release）のカーネル内に実装した．試作システムの実装方式を図 7 に示す. IP 層で行われる既存の処理に一切の変更を加えず，カーネル空間の関数である ip_input(), ip_output()で PCCOM モジュールに処理を渡し，処理を終えたら差し戻す．PCCOM はパケットフォーマットを変えずに処理する方式であるため，この様な方式を容易に実現できる上，高スループットを発揮できるという利点がある．一方，IPsec はヘッダの追加などパケットフォーマットに変更があるため，IP 層全体に渡って処理の変更が必要となる．

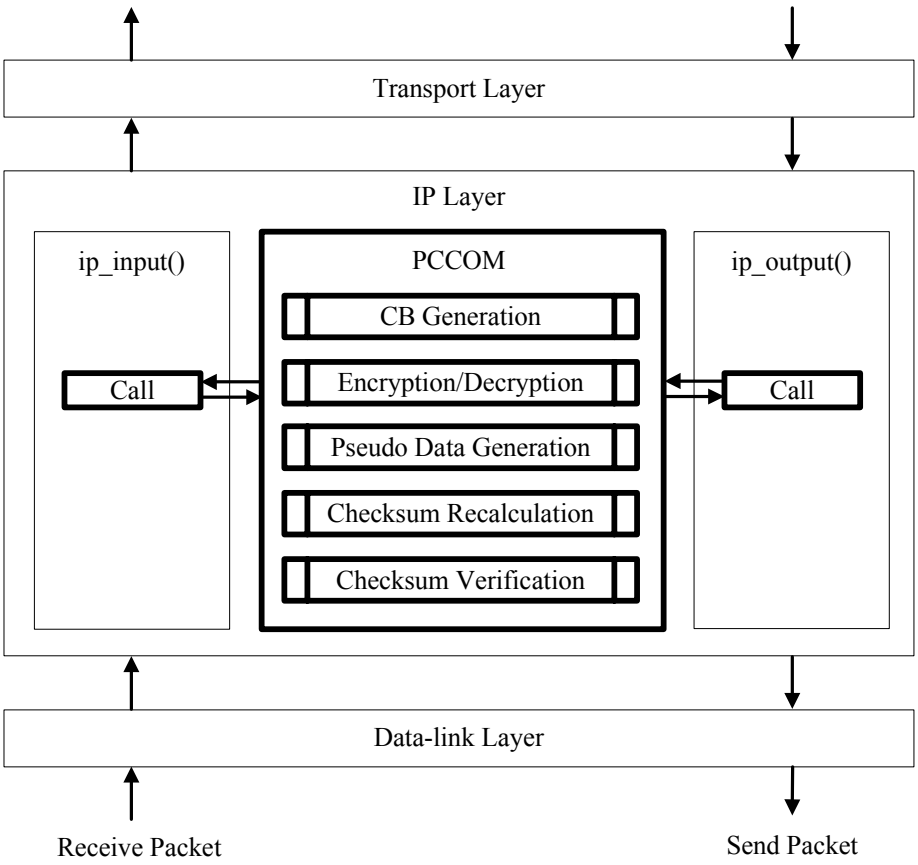


図 7　試作システムの実装方式

Fig.7　Implementation method of the trial system.

4.2. システムの仕様・構成と動作概要

試作システムの仕様を表 1 に示す. 動作処理情報テーブルはハッシュテーブルとして実装する. 暗号アルゴリズムは AES（鍵長は 128 ビット）を採用し，ハッシュ関数は MD5 を用いた. なお, 暗号ライブラリとして OpenSSL（openssl-0.9.7d）[12)]を採用した.

表 1　試作システムの仕様

Table 1　Specification of the trial system.

項　　目	内　　容
テーブル検索方式	ハッシュ法
暗号アルゴリズム	AES（CFB モード）
鍵長	128 ビット
ハッシュ関数	MD5

PCCOM モジュールは主処理とサブモジュールから構成される．主処理ではテーブル検索処理や各サブモジュールを呼び出す処理を行う．サブモジュールは，CB 生成モジュール，暗号化/復号モジュール，疑似データ生成モジュール，チェックサム再計算モジュール，チェックサム検証モジュールから構成される．PCCOM モジュールは通信パケットに対し，予め作成済みの動作処理情報テーブルに基づき処理を実行する．動作処理情報テーブルには IP アドレス，ポート番号，プロトコル番号と，それに対応する動作内容，すなわち暗号化/復号，透過中継，廃棄などが記されている．ip_input()，ip_output()で PCCOM モジュールが呼び出されると，送受信パケットの IP アドレス，ポート番号，プロトコル番号から算出したハッシュ値で，該当する動作処理情報を検索し，テーブル内容に正しい IP アドレス，ポート番号，プロトコル番号が存在することを確認する．その後，テーブルに記された動作内容に応じて対応する処理を行う.

試作システムを用いて，パケットフィルタリングタイプのファイアウォールおよび NAT を中継して通信できることを確認し，パケットの内容を書き換えた場合，不正パケットとして検出できることを確認した.

5. 評　価

5.1. 試作システムの性能評価

試作システムを実装した 2 台の端末間の通信性能を測定した．参考のために IPsec ESP（KAME[13]）を実装した場合を測定し比較した．また，PCCOM 内部の処理時間をモジュール別に測定し，処理のネックとなっている部分を明らかにした．実験に用いた端末の仕様を表 2 に示す．IPsec の設定は，試作システムの仕様と条件が同じになるように，ESP トランスポートモードで，暗号アルゴリズムは AES（鍵長は 128 ビット），認証アルゴリズムは HMAC-MD5 とし，リプレイ防御機能は OFF とした．

表 2　実験端末の仕様

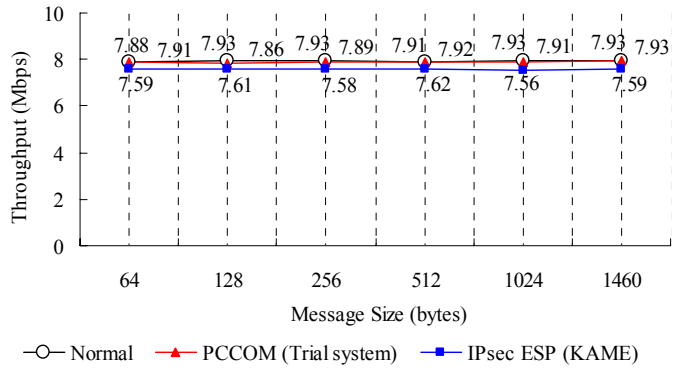
Table 2　Specifications of the terminals.

項　目	内　容
CPU	Pentium4 2.4GHz
Memory	256MB
NIC	10BASE-T,100BASE-TX,1000BASE-TX
OS	FreeBSD (5.3 Release)

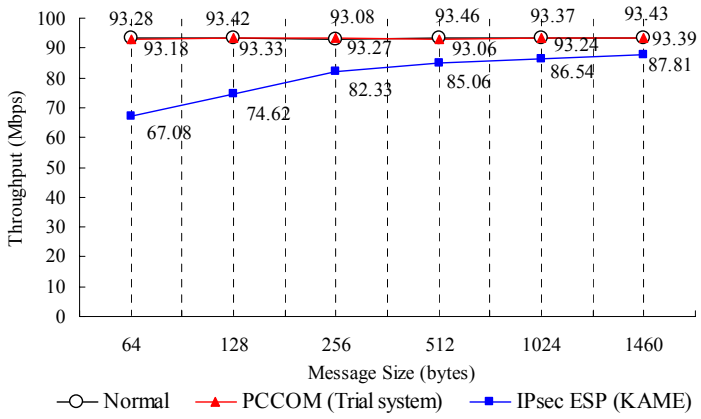
5.1.1. 通信性能の測定

図 8 は IP パケット長とスループットの関係を，10BASE，100BASE，1000BASE の通信環境ごとに，暗号化をしない場合（以下，Normal と呼ぶ），PCCOM の場合，IPsec ESP の場合のそれぞれについて示したものである．スループットの測定にはネットワークベンチマークソフト Netperf[14]を用いて，10 回試行の平均値をとった．

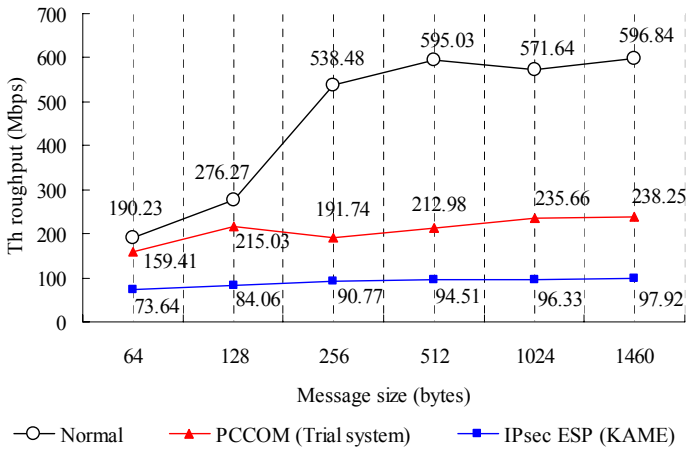
10BASE の環境では，ESP においては若干の性能低下が見られたものの，処理すべきパケット数が少ないため，PCCOM，ESP とも処理オーバヘッドはネックとなっていない．100BASE の環境では，Normal と PCCOM は NIC の上限性能を発揮しており PCCOM に性能低下は見られなかった．それに対し ESP はメッセージサイズ 1460 バイトのパケット（以下，長パケットと呼ぶ）では Normal から約 6%性能が低下しており，メッセージサイズ 64 バイトのパケット（以下，短パケットと呼ぶ）では約 28.1%低下している．また 1000BASE の環境では，長パケッ



(a) 10BASE environment



(b) 100BASE environment



(c) 1000BASE environment

図 8　スループット測定結果

Fig.8　Measurement results of throughput.

トの場合 PCCOM は Normal から約 60.1%性能が低下しており，ESP では約 83.6%低下している．短パケットの場合 PCCOM は Normal から約 16.2%性能が低下しており，ESP では約 61.3%低下している．

パケットサイズが短くなるほどスループットが落ち込むのは，相対的に処理すべきパケット数が多くなるので，ソフトウェアによるオーバヘッドの占める割合が大きくなるためである．とりわけ ESP の短パケットでは，ヘッダの追加など暗号化以外の処理ネックが顕著に現れているといえる．

次に，1000BASE の環境において，FTP で 500MB のファイルをダウンロードするのに要した時間を図 9 に示す．測定結果は 10 回試行の平均値である．PCCOM は Normal の約 145.1%の時間であるのに対し，ESP は約 311.6%の時間を要している．

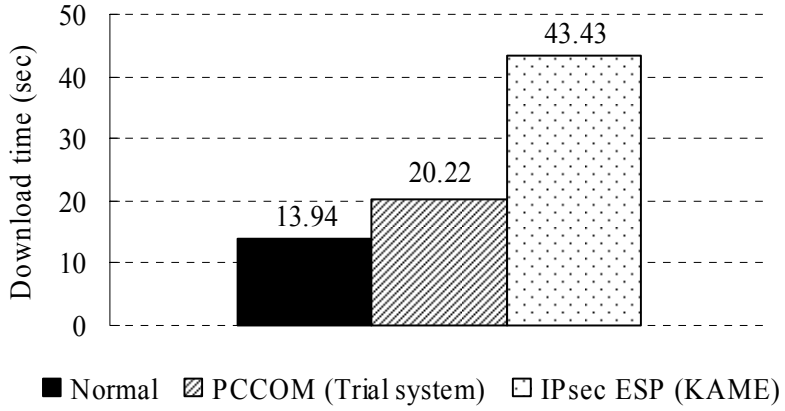


図 9　500MB ファイルの FTP ダウンロード時間

Fig.9　Download time of a 500MB file using FTP.

5.1.2. PCCOM 内部の処理コスト

PCCOM における処理過程での処理コストを調べるために PCCOM の内部処理時間をモジュール別に測定した．内部処理時間は，RDTSC （ReaD Time Stamp Counter）を用いて処理前後の CPU クロックカウンタ値を求めて算出した．

PCCOM 内部の処理時間とそれぞれの比率を表 3 に示す．表 3 の主処理とは，PCCOM モジュールが呼ばれたときに最初に実行される処理で，主処理の中で動作処理情報テーブルの検索が実行され，その結果に基づいて各サブモジュールが呼び出される．測定結果は FTP の通信中に流れた IP データグラム長 1460 バイト

表 3　PCCOM 内部の処理時間とそれぞれの比率

Table 3　Internal processing time of the PCCOM and each ratio.

	測定対象	処理時間（μs）	比率（%）
送信側	主処理（テーブル検索以外）	0.547	1.8
	主処理（テーブル検索）	0.268	0.9
	CB 生成	0.868	2.9
	暗号化	26.043	87.6
	疑似データ生成	1.704	5.7
	チェックサム再計算（独自）	0.294	1.0
受信側	主処理（テーブル検索以外）	0.545	1.7
	主処理（テーブル検索）	0.269	0.8
	CB 生成	0.890	2.8
	疑似データ生成	2.863	9.0
	チェックサム検証（独自）	0.281	0.9
	復号	25.547	80.6
	チェックサム再計算（通常）	1.286	4.1

のパケット 10 個の結果の平均値である．表 3 より，送信側，受信側ともに暗号化/復号が処理の 8 割以上を占めていることが分かる．専用のハードウェア暗号エンジンを用いるなどで，処理時間の大幅な短縮が期待でき，より Normal に近い性能を発揮できると考えられる．また，動作処理情報テーブルの検索処理は約 0.27μs と PCCOM 全体の約 1%程度であり，検索処理のオーバヘッドは問題とならない．

PCCOM はパケットフォーマットを変えないため，メモリバッファに蓄積されたパケットの暗号化/復号などの処理をそのままの位置で実行することができる．暗号化/復号以外の処理としてはチェックサムの再計算などが挙げられるがそれらの処理は大きなものではない．一方，IPsec ではヘッダの追加処理などを伴うので暗号化/復号以外の処理が多く，オーバヘッドも大きくなる．

5.2. PCCOM の安全性

PCCOM が提供する機能はデータの機密性確保，本人性確認，パケットの完全性保証である．その上で考えられる脅威を以下に述べる．

PCCOM では IP ヘッダ，TCP/UDP ヘッダが平文であるためトラフィックの内

容を解析される恐れがあるが，ファイアウォールの通過を可能とするにはヘッダ部分がファイアウォールに見えることが必須である．すなわち，ファイアウォールのパケットフィルタリングを可能にすることとトラフィック解析を不可とすることを同時に満足させることはできない．PCCOM は前者に重点を置くシステムを対象とする場合に有効である．

PCCOM では認証値がチェックサムフィールド長 16bit であるため，$1/2^{16}$ の確率でパケットの偽造や完全性保証範囲のフィールドの改竄に成功する．パケットの偽造を利用した代表的な攻撃として TCP セッションハイジャックが考えられるが，ハイジャックを成功させるには，通信を中断させる RST パケット，再接続の SYN パケットとその SYN/ACK に対する ACK パケットの，3 ステップのパケットの偽造を成功させる必要があるため，実際にハイジャックに成功する確率は極めて低い．また，仮にハイジャックに成功したとしても，ユーザデータは暗号化範囲であるため意図したデータを送ることはできない．また，ユーザデータは暗号化されているため意図した改竄は困難である．仮にユーザデータ部分が改竄された場合，受信側で行う復号の結果が予期せぬ値となり，多くのアプリケーションではエラー処理により廃棄される．また，音声などのストリーミングのパケットは，改竄されて予期せぬ復号結果となった場合はノイズとして扱われる．

PCCOM では，IP アドレスとポート番号は NAT を経由する際に値が変化するため完全性保証の範囲に含めていない．これらの完全性は，パケットの処理内容を記述した動作処理情報テーブルの検索過程で保証する．従って，通信経路上で送信元アドレスの改竄や，ポート番号の改竄によるアプリケーションの誤作動などを招く行為を防ぐことができる．

動作処理情報テーブルはカーネル内に保存されるため，カーネルをハックされない限りその内容を改竄することは困難である．またテーブルを生成する際には，両端末間の確実な認証を必要とするため，誤った情報登録の可能性は低いと考えられる．

5.3. IPsec ESP とのすみわけ

IPsec ESP と PCCOM を 7 項目において定性的に比較した結果を表 4 に示す．

IPsec ESP は，高い機密性と強力な認証機能を提供しているが，TCP/UDP ヘッダの暗号化や完全性保証が原因で NAT やファイアウォールと共存することができない．また，ヘッダの追加によるオーバヘッドやフラグメントが発生する．

PCCOM は，パケットフォーマットを変えないまま本人性確認とパケットの完全性保証を実現しており，NAT やファイアウォールと共存することができる．また，フラグメントが発生せず，高スループットを実現できるというメリットがある．暗号化範囲はポート番号によるフィルタリングを可能とするためユーザデー

表 4　IPsec ESP との比較.

Table 4　Comparison with IPsec ESP.

	IPsec ESP	PCCOM
機密性	Excellent	Good
本人性確認	Excellent	Good
完全性保証	Excellent	Good
NAT	Poor	Good
ファイアウォール	Poor	Good
フラグメント	Poor	Good
トラフィック解析	Good	Poor

タ部分のみとしているが，本人性確認・完全性保証の実現により TCP/UDP ヘッダが平文であることによる安全性低下を防止している．IP ヘッダ，TCP/UDP ヘッダは平文であるため，トラフィック解析をされる懸念があるが，ファイアウォールのパケットフィルタリングによって，管理者が許可した用途のパケットのみを通過させることができるという利点がある．

IPsec ESP は，強靭なセキュリティを必要とする部門への適用が適しており，通信経路上に NAT やファイアウォールが存在してはいけない．また，スループットの低下が問題とならないことを確認する必要がある．用例としては，イントラネット内部でも特に強靭なセキュリティを要する部門や，インターネット上で拠点間通信などの重要データの取引が行われるような環境に適している．それに対し PCCOM は，NAT やファイアウォールとの共存が可能で，高スループットを実現できるなどの理由で，比較的広範囲への適用が可能と考えられる．用例としては，高スループットを要するアプリケーションの通信形態として多い P2P 通信や，パケットフィルタリングタイプのファイアウォールを備えたホームネットワークへのアクセス，部門ごとにファイアウォールを設置している場合が多いイントラネット内の通信に有効と考えられる．

6. ま と め

NAT やファイアウォールと共存でき，オリジナルパケットのフォーマットを変えないまま，本人性確認とパケットの完全性保証を行うことができる暗号通信方式 PCCOM を提案した．PCCOM は本人性確認と IP アドレス・ポート番号を除く

パケットの完全性保証を，共通秘密鍵とパケットの内容から生成した疑似データと呼ぶ値を用いて，TCP/UDP チェックサムを再計算することにより実現する．また，IP アドレスとポート番号については動作処理情報テーブルを検索する過程でその内容を保証する．PCCOM の有効性を確認するために試作システムを実装し，動作検証を行った．性能測定の結果，高スループットが得られることを確認した．また，PCCOM の安全性について考察し，IPsec ESP とのすみわけが可能であることを示した．

謝　　辞

本研究に関して，研究の方向性や進め方など多大なる御指導，御鞭撻を賜りました名城大学理工学部情報工学科 渡邊晃教授に心より厚く御礼申し上げます．

本研究を進めるにあたり，様々な御助言，御検討を頂ました名城大学理工学部情報工学科 小川明教授に心より厚く御礼申し上げます．

本研究を進めるにあたり，様々な御助言，御検討を頂ました名城大学理工学部情報工学科 柳田康幸教授に心より厚く御礼申し上げます．

本研究を進めるにあたり，様々な御助言，御検討を頂ました名城大学理工学部情報工学科 宇佐見庄五講師に心より厚く御礼申し上げます．

本研究を進めるにあたり，様々な御助言，御検討を頂きました宮崎大学工学部情報システム工学科 岡崎直宣助教授に心より厚く御礼申し上げます．

最後に，本研究を進めていく上で様々な御励まし，御助言，御検討を頂きました名城大学理工学部情報工学科渡邊研究室の皆様に心より感謝いたします．

参 考 文 献

1) S. Kent and R. Atkinson “Security Architecture for the Internet Protocol,” RFC2401, Aug. 1998.

2) R. Atkinson, “IP Authentication Header,” RFC2402, Dec. 1998.

3) R. Atkinson, “IP Encapsulation Security Payload (ESP),” RFC2406, Dec. 1998.

4) D. Harkins and D. Carrel, “The internet key exchange (IKE),” RFC2409, Dec. 1998.

5) A. Huttunen, B. Swander, V. Volpe, L. Diburro, and M. Stenberg, “UDP Encapsulation of IPsec Packets,” RFC3948, Jan. 2005.

6) Y. Zhang and B. Singh, “A Multi-Layer IPsec Protocol,” Proc. 9th USENIX Security Symposium, Aug 2000.

7) 渡邊晃，厚井裕司，井手口哲夫，横山幸夫，妹尾尚一郎，“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”，情処学論， vol.38, no.4, pp.904-914, Apr 1997.

8) R. Braden, D. Borman, and C. Partridge, “Computing the Internet Checksum,” RFC1071, Sep. 1988.

9) T. Mallory and A. Kullberg, “Incremental Updating of the Internet Checksum,” RFC1141, Jan. 1990.

10) A. Rijsinghani, “Computation of the Internet Checksum via Incremental Update,” RFC1624, May. 1994.

11) K. Egevang and P. Francis, “The IP Network Address Translator (NAT),” RFC1631 May. 1994”.

12) OpenSSL Project, http://www.openssl.org/

13) KAME Project, http://www.kame.net/

14) Netperf, http://www.netperf.org/

研 究 業 績

1. 学術論文

増田真也，鈴木秀和，岡崎直宣，渡邊晃，“NAT やファイアウォールと共存できる暗号通信方式 PCCOM の提案と実装”，情報処理学会論文誌（条件付採録）

2. 国際会議

Shinya Masuda, Hidekazu Suzuki, Naonobu Okazaki and Akira Watanabe, “Proposal for a Practical Cipher Communication Protocol that Can Coexist with NAT and Firewalls,” The International Conference on Information Networking 2006, Jan. 2006.

3. 口頭発表

1) 増田真也, 渡邊晃,“閉域通信グループにおける暗号通信方式の検討”，電気関係学会東海支部連合大会，Oct. 2003.

2) 増田真也, 渡邊晃,“閉域通信グループにおける暗号通信方式の検討”，第 66 回　情報処理学会全国大会，Mar.2004.

3) 増田真也，渡邊晃，“実用性を重視した暗号通信方式の提案”，情処研法，2004-CSEC-26, pp.267-274, Jul. 2004.

4) 増田真也，渡邊晃，“実用暗号通信 PCCOM の実装と評価”，情処研法，2004-CSEC-28, pp.205-210, Mar. 2005.

5) 増田真也，鈴木秀和，渡邊晃，“IPv4/IPv6 混在環境における暗号通信方式の考察”，マルチメディア，分散，協調とモバイル（DICOMO2005）シンポジウム（査読付き），pp.693-696, Jul.2005.

6) 大石泰大，増田真也，渡邊晃，“WAPL を適用した車車間通信の実現”，マルチメディア，分散，協調とモバイル（DICOMO2005）シンポジウム（査読付き），pp.153-156, Jul.2005.

7) 加藤佳之，大石泰大，増田真也，渡邊晃，“WAPL とインターネット接続に関する検討”，電気関係学会東海支部連合大会，Sep. 2005.

4. 表彰

情報処理学会全国大会 学生奨励賞
増田真也，渡邊晃，“閉域通信グループにおける暗号通信方式の検討”，第 66 回　情報処理学会全国大会，Mar.2004.

付　録

A　PCCOM 仕様書（抜粋版）

PCCOM を実装するにあたり，仕様書を作成したので付録として添付する．

PCCOM 仕様書（抜粋版）

著者：増田 真也 （マスダ シンヤ） 名城大学大学院理工学研究科情報科学専攻
監修：渡邊 晃 （ワタナベ アキラ）名城大学理工学部情報工学科 教授

最終更新日：2006 年 2 月 3 日

1. はじめに

PCCOM（Practical Cipher COMmunication protocol）は，FPN（Flexible Private Network）を構築するためのネットワークセキュリティアーキテクチャ GSCIP（Grouping for Secure Communication for Internet Protocol；ジースキップ）において，GE（GESCIP Element）の機能を実現するためのモジュール郡を取りまとめた GPACK（GSCIP PACKage）の一機能である．PCCOM は GPACK メインモジュールから呼び出されて処理する．

PCCOM は，安全な通信を行うために，パケットの暗号化/復号，送信元の本人性確認，パケットの完全性保証を行う．

本仕様書に関連するドキュメントの一覧を表 1-1 に示す．

表 1-1 関連ドキュメント

ドキュメント名	内容
FPN システム説明書	FPN の概念について記した説明書 （HP；http://www.wata-lab.meijo-u.ac.jp/research/fpn1.html）
GSCIP 基本設計書	FPN を構築するためのセットワークセキュリティアーキテクチャ GSCIP の基本設計書
GPACK Main Module 仕様書	GPACK メインモジュールの仕様書
DPRP 仕様書	事前交渉プロトコル DPRP の仕様書
SPAIC 仕様書	セキュア鍵配送プロトコル SPAIC の仕様書
GPIT 仕様書	動作処理情報テーブル GPIT の定義と動作を記した仕様書
mbuf 説明書	FreeBSD のメモリバッファについて説明したドキュメント

2. 機能

本モジュールが提供する各機能を以下に示す.

2.1. パケットの暗号化/復号

パケットの盗聴から保護するために，始点/終端の GE で暗号化/復号を行う.

2.1.1. 暗号化範囲

暗号化範囲は図 2-1 のように規定することで，既存システムに影響を与えないようにする.

RIP，OSPF はルータ間の経路制御に使用するので暗号化しない．ICMP はエラー発生時，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したりするので暗号化しない．DHCP はアドレスの割り当てに使用するため暗号化しない．ARP はアドレス解決のために暗号化しない．TCP/UDP は NA(P)T やファイアウォールの通過のために暗号化しない.

TCP/UDP による一般通信は，ユーザデータが暗号化された状態である.

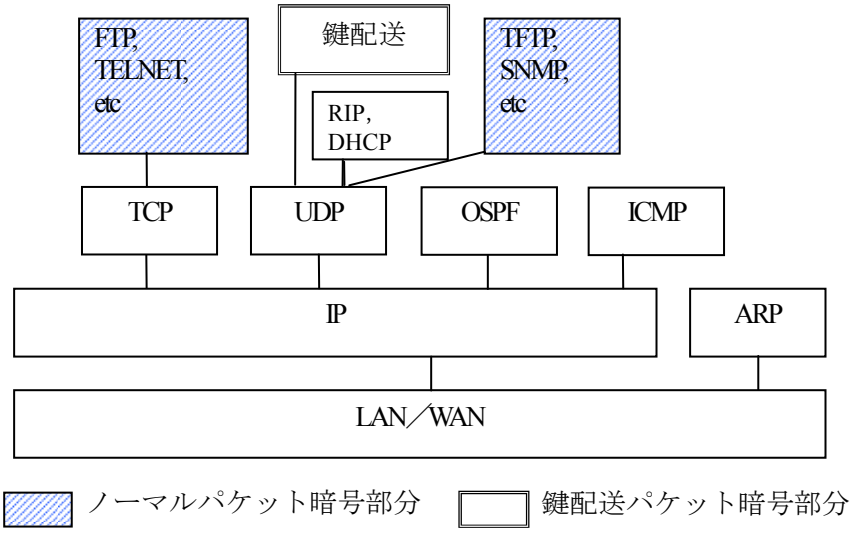


図 2-1　TCP/IP パケットの暗号化範囲

暗号化/復号を行うパケットの判別は GPACK にて行うので，本モジュールでは呼び出し時に渡された動作処理情報構造体の情報を元に暗号化/復号を行う.

2.1.2. 暗号方式

暗号方式は本方式である PCCOM で，平文と暗号文をそのまま置き換える．この手段としてブロック暗号の CFB（Cipher FeedBack）モード※を用いる．これにより，オリジナルパケットと全く同じサイズの暗号化が実現できる．よって，提案方式によるオーバヘッドやフラグメントはなく，高スループットを実現できる.

※ CFB モード
ブロック暗号をストリーム暗号として利用するモード．ストリーム暗号として RC4 などが挙げられるが，実装上ブロック暗号の方が普及しており，ブロック暗号はハードウェア化が容易で安価な暗号チップが手に入り安いことから，ブロック暗号の CFB モードを採用した．類似モードに OFB モードがあるが，セキュリティの面で CFB の方が強力である.

2.2. 本人性確認とパケットの完全性保証

安全な通信を行う上で，パケットの盗聴を防止する以外に，送信元が正当な相手であることの保証やパケットが改竄されていないことを保証することが重要である．前者を本人性確認，後者をパケットの完全性保証と呼ぶ.

本モジュールでは TCP/UDP のチェックサムを用いることで, パケット長を変えないまま本人性確認と完全性保証を行う．CB（Checksum Base）と呼ぶチェックサムベース値を定義し，CB と暗号データのハッシュ値から生成した疑似データと呼ぶ値を用いて計算した TCP/UDP チェックサムによって本人性確認と完全性保証を実現する.

2.2.1. CB (Checksum Base) の生成

CB は，IP ヘッダ，TCP/UDP ヘッダで転送中に値の変化しないフィールドと，事前に秘密裏に共有している共通秘密鍵を含めた値から生成したハッシュ値である. CB の種には共通秘密鍵の他にシーケンス番号のように初期値が乱数で決まりパケットごとに値が変化するフィールドを含んでおり，CB 値を第三者が推測するのは極めて困難である．CB 生成に用いるフィールドを図 2-3 に示す※.

なお，暗号化で必要な初期値 IV（Initialization Vector）には CB 値を流用する.

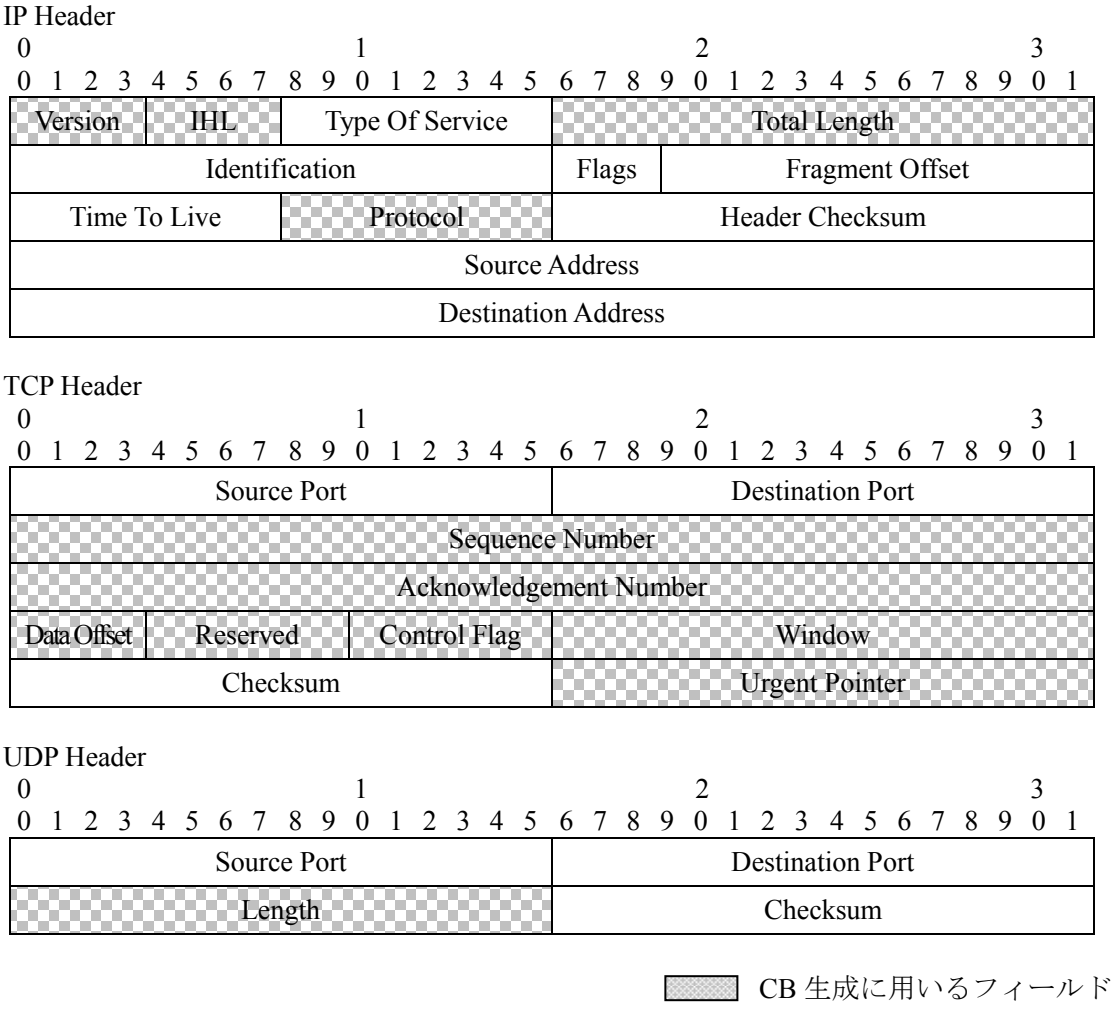


図 2-3　CB 生成に用いるフィールドの範囲※

※ 本仕様書では IP オプションは考慮していない

2.2.2. 疑似データによる TCP/UDP チェックサムの再計算/検証

前節の手順で生成した CB を TCP/UDP チェックサムの再計算/検証に用いる．一般通信と PCCOM の, TCP/UDP チェックサムの計算範囲の違いを図 2-4 に示す. 一般の通信では, TCP/UDP チェックサムは TCP/UDP ヘッダ，TCP/UDP 疑似ヘッダ，ユーザデータから計算される．一方 PCCOM では，TCP/UDP チェックサムは TCP/UDP ヘッダ，TCP/UDP 疑似ヘッダ，疑似データから計算される．ここで，疑似データとは暗号データと CB を元に求めたハッシュ値である．送信側ではデータの暗号化後，疑似データを用いて TCP/UDP チェックサムの再計算を行う．受信側ではデータの復号を行う前に，同様の方法で生成した疑似データによって計算したチェックサムを検証する．検証結果が正常であれば，復号を行いオリジナルチェックサムの再計算を行って上位層（TCP/UDP）に渡す．この方式により，暗号データと CB 生成に用いたフィールドの完全性を保証することができると同時に本人性確認も実現される．

パケットの改竄者が改竄を隠蔽するために，パケットの一部を書き換えると同時に TCP/UDP チェックサムを再計算しようとしても，疑似データの内容が分からないので正しい計算を行うことはできない．なお，IP アドレスとポート番号の保証方法については次節で述べる．

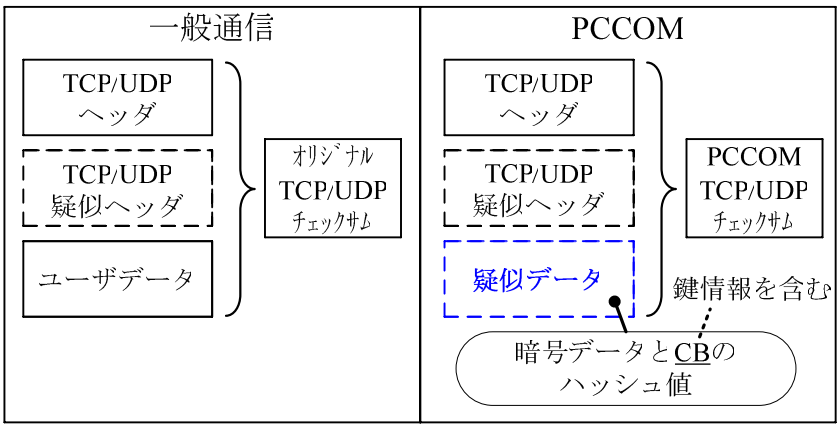


図 2-4　チェックサム計算範囲の違い

2.2.3. DPRP と組み合わせたパケットの完全性保証

PCCOM では，IP アドレスとポート番号は NAT を経由する際に値が変化するため CB 生成の範囲に含めいていない．これらの完全性保証は，パケットの処理内容を記述した動作処理情報テーブルの検索過程で保証する．テーブル検索の処理を図 6 に示す．動作処理情報テーブルには，送信元と宛先の IP アドレスとポート番号，プロトコル番号とそれに対応する，パケットの処理内容（暗号化/復号，透過中継，廃棄），共通秘密鍵の識別情報（グループ番号，鍵バージョン）が記述されている. 送信側と受信側の両端末は通信の開始前に設定情報の交換を行い，通信パケットの処理に必要となる動作処理情報を生成して動作処理情報テーブルに保存する．送信側の端末はパケットの送信時に, 受信側の端末はパケット受信時に, パケットの IP アドレス，ポート番号，プロトコル番号を元に動作処理情報テーブルを検索し，テーブル内に該当パケットの動作処理情報が存在する場合はその情報に応じてパケットを処理する．従ってテーブル検索後，テーブルの内容から IP アドレス，ポート番号，プロトコル番号を再度確認し，テーブル内に該当パケットの情報が正しく存在したら，IP アドレスとポート番号は改竄されていなかったことが保証される．

この方式は事前に正しい内容のテーブルが生成されていることが前提となる．本仕様では，事前交渉プロトコル DPRP（Dynamic Process Resolution Protocol）※を用いている．

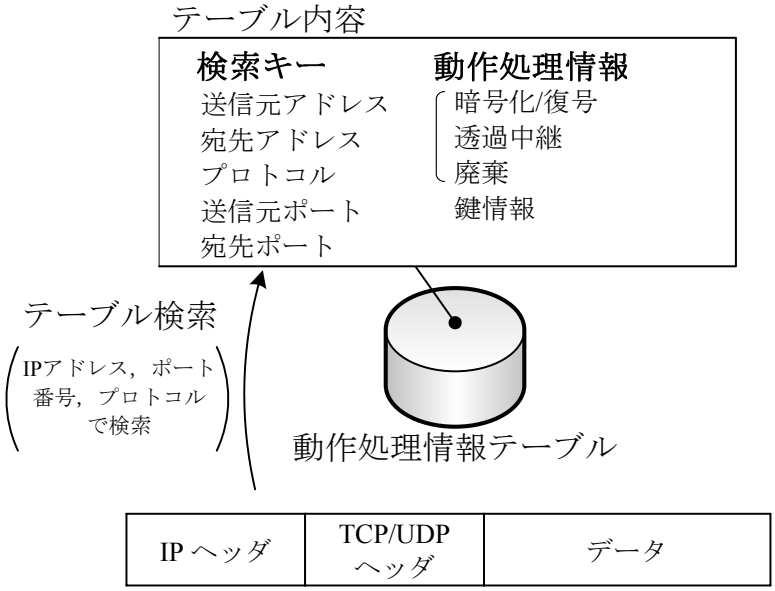


図 2-5　テーブル検索処理

※現状の DPRP は NA(P)T を通過できないが，将来的に通過可能となった場合を想定している．

3. 仕様

本モジュールの仕様は，表 3-1 のとおりである．

表 3-1　仕様

項目	内容
暗号アルゴリズム	AES (CFB モード)
鍵長	128 ビット，192 ビット，256 ビット※1
暗号化範囲	図 2-1 参照
ハッシュ関数	MD5 ※2
CB 生成に用いるフィールド	図 2-3, 2-4 参照

※ 1　鍵長
デフォルトは 128 ビット．本来なら設定で判断すべき
※ 2　MD5
特定の条件下衝突サーチ攻撃に対して弱いことが報告されているが，本モジュールの本質的な問題ではないので，AES_CFB に用いる IV のサイズと同じ 128bit 出力である MD５を使用する．

4. 内部構成

4.1. モジュール構成

PCCOM は，表 3-1 のようにメインモジュールである PCCOM モジュールと，サブモジュールである CB 生成モジュール，暗号化/復号モジュール，疑似データ生成モジュール，チェックサム再計算モジュール，チェックサム検証モジュールから構成される．

表 3-1　モジュールの構成と機能

モジュール	機能
PCCOM	メインモジュール．各サブモジュールを呼び出し，一連の処理を組み立てる．
CB 生成	IP ヘッダ，TCP/UDP ヘッダで転送中に変化しないフィールドと暗号鍵を合わせたハッシュを生成する．
暗号化/復号	入力データをブロック暗号の CFB モードで暗号化/復号する．
疑似データ生成	暗号データと CB を合わせたハッシュを生成する．
チェックサム再計算	通常または疑似データを含めた独自の計算範囲でチェックサムの再計算を行う．
チェックサム検証	通常または擬似データを含めた独自の計算範囲でチェックサムの検証を行う．

4.2. ファイル構成

PCCOM は表 4-1 に示すファイルから構成される.

表 4-1　ファイル構成

ファイル	場所	内容
pccom.h	/sys/netgscip/	PCCOM ヘッダ
pccom.c	/sys/netgscip/	PCCOM ソース

4.2.1. マクロ定数（pccom.h）

表 4-2　マクロ定数

定数	値	説明
IV_LEN	16	IV のサイズ（バイト）
CB_LEN	IV_LEN	CB のサイズ（バイト）
SUM_TRUE	1	チェックサム検証結果が真
SUM_FALSE	0	チェックサム検証結果が偽
CKSUM_PSEUDO	1	疑似データを用いたチェックサム計算
CKSUM_NORMAL	0	通常のチェックサム計算
PCCOM__DISCARD	1	廃棄
PCCOM__DONE	0	正常に処理を完了

4.2.2. 関数（pccom.c）

4.2.2.1. PCCOM

int pccom(struct ip *ip, char *nxthdr, struct mbuf *m1, PID *gpie)

機能:
　暗号処理モジュール
パラメータ:
　ip　　: IP ヘッダ構造体のアドレス (I)
　nxthdr　　: 上位ヘッダ(TCP/UDP)構造体のアドレス (I/O)
　m1　　: mbuf 構造体※のアドレス（I/O）
　pid　　: 動作処理情報構造体のアドレス (I)
戻り値:
　PCCOM_DISCARD（1）　: 破棄
　PCCOM_DONE（0）　: 正常

※ mbuf 構造体
FreeBSD のメモリバッファ　詳細は「mbuf 説明書」を参照.

4.2.2.2. CB 生成

int make_cb(struct ip *ip, char *nxthdr, u_char * key, u_char *cb)

機能:
CB 生成モジュール
パラメータ:
ip : IP ヘッダ構造体のアドレス (I)
nxthdr : 上位ヘッダ(TCP/UDP)構造体のアドレス (I)
key : 鍵のアドレス (I)
cb : CB のアドレス (I/O)
戻り値:
PCCOM_ DISCARD（1） : 破棄
PCCOM_ DONE（0） : 正常

4.2.2.3. 暗号化/復号

void crypto(u_char *idat, int ilen, u_char *key, u_char *iv, int *num, int EncDec)

機能:
暗号化/復号モジュール (AES_CFB)
パラメータ:
idat : 入力データのアドレス (I/O)
ilen : 入力データ長 (I)
key : 鍵のアドレス (I)
iv : IV のアドレス (I/O)
num : num※のアドレス (I/O)
EncDec : AES_ENCRYPT(1) 暗号化
AES_DECRYPT(0) 復号 (I)
戻り値:

※ num について.
GPACK において送信時呼び出しではユーザデータ長が 209 バイト以上の場合，mbuf のデータは分割されてチェーンで連結されている．すると，ユーザデータを暗号化する時にそれぞれの分割データを処理する必要がある．ここで注意すべき点は，受信側ではこのユーザデータが 1 つに繋がった状態であるということである．すなわち，送信側で，分割されたデータをそれぞれ暗号化したものが受信側では繋がっていて，それを復号しなければならないということだ.
一般的にブロック暗号は，ブロック長（AES なら 16 バイト）の整数倍のデータ長しか扱うことができない．例えば，64 バイトのデータがあって，32 バイトと 16 バイトに分割されたデータをそれぞれ暗号化して，結合したものをまとめて復号することはできるが，30 バイトと 34 バイトという様にブロック長の整数倍でない場合は，ブロックサイズになるように 30 バイトデータには 2 バイトのパディングを，34 バイトデータには 14 バイトのパディングをする必要がある．この場合は 80 バイト（32+48）のデータを復号することになる．これではパケット長が大きくなってしまう．しかし CFB モードであればその問題はない.
そこで用いられるのが num で，呼び出し時は通常 0 を与える．上記のようにデータが分割されていて，それを暗号化したあとに結合されたデータを復号する場合は，例えばデータが 2 分割されている場合，暗号化のときに前方の分割データを暗号化するときには num の入力値は 0 だが, 後方の分割データを暗号化するときには，前方で呼び出されたときの最終的な num の値をそのまま入力して処理する.

4.2.2.4. 疑似データ生成

int make_pseudo_data(u_char *ip, char *nxthdr, struct mbuf *m, u_char *cb, u_char *pseudo)

機能:
　擬似データ生成モジュール
パラメータ:
　ip　　: IP ヘッダ構造体のアドレス (I)
　nxthdr　　: 上位ヘッダ(TCP/UDP)構造体のアドレス (I)
　m　　: mbuf 構造体のアドレス（I）
　cb　　: CB のアドレス (I)
　pseudo　　: 疑似データのアドレス (I/O)
戻り値:
　PCCOM_ DISCARD（1）　: 破棄
　PCCOM_ DONE（0）　　: 正常

4.2.2.5. チェックサム再計算

void recalc_cksum(struct ip *ip, char *nxthdr, struct mbuf *m, u_char *pseudo, int mode)

機能:
　チェックサム再計算モジュール
パラメータ:
　ip　　: IP ヘッダ構造体のアドレス (I)
　nxthdr　　: 上位ヘッダ(TCP/UDP)構造体のアドレス (I/O)
　m　　: mbuf 構造体のアドレス（I）
　pseudo　　: 疑似データのアドレス (I)
　mode　　: CKSUM_NORMAL(0)　　通常のデータによる計算
　　CKSUM_PSEUDO(1)　　疑似データによる計算 (I)
戻り値:

4.2.2.6. チェックサム検証

int verify_cksum(struct ip *ip, char *nxthdr, struct mbuf *m, u_char *pseudo)

機能:
　チェックサム検証モジュール
パラメータ:
　ip　　: IP ヘッダ構造体のアドレス (I)
　nxthdr　　: 上位ヘッダ(TCP/UDP)構造体のアドレス (I)
　m　　: mbuf 構造体のアドレス（I）
　pseudo　　: 疑似データのアドレス (I)
戻り値:
　SUM_TRUE(1)　　: 正しい
　SUM_FALSE(0)　　: 誤りがある

4.3. 各モジュールの処理フロー

4.3.1. PCCOM（概略版）

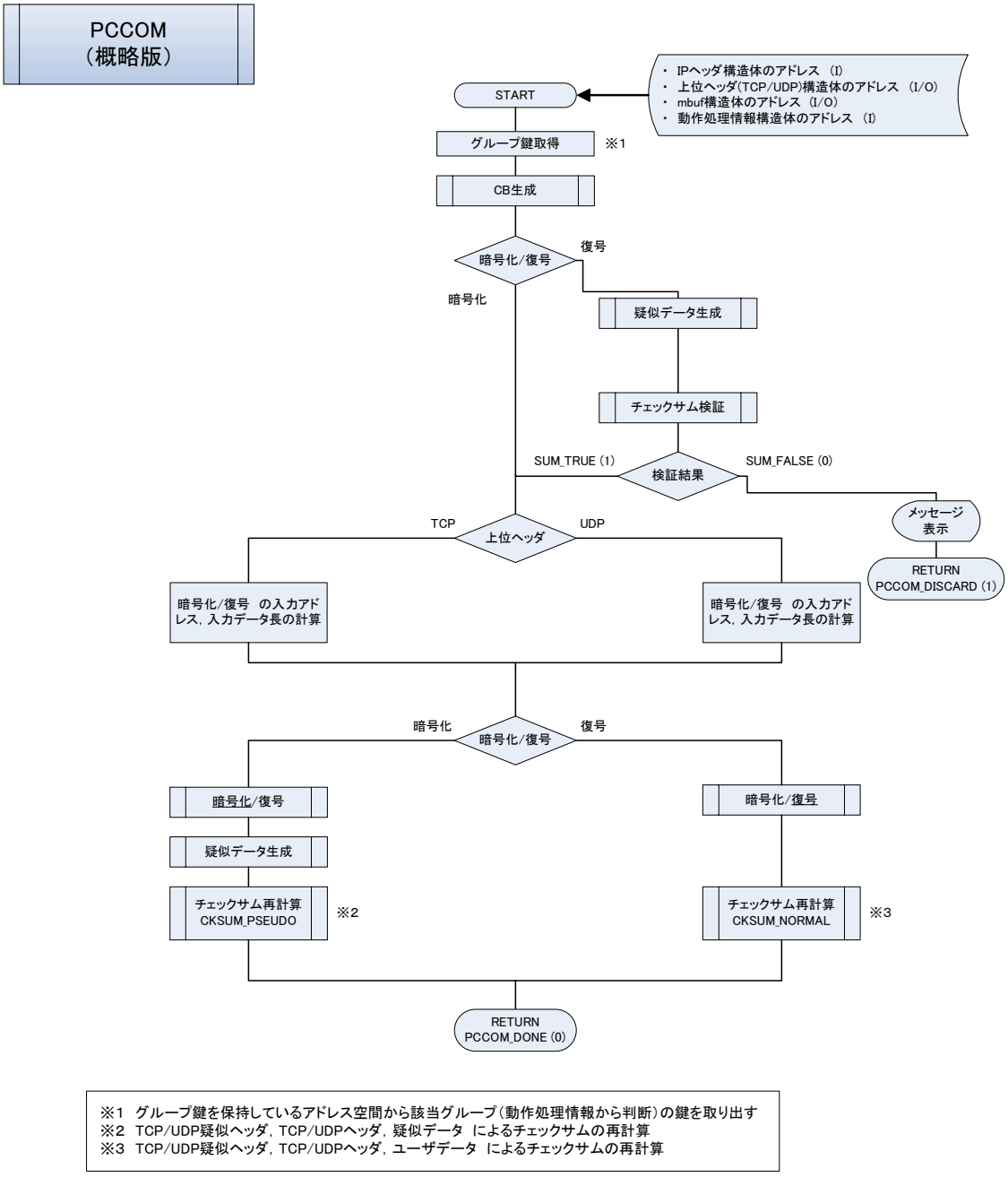


図 4-1 PCCOM モジュールの概略フロー

図 4-1 は，全体の概略を把握するためのものである．以降は実際のプログラムの流れに沿った詳細のフローチャートを載せている．

B　GSCIP 基本設計書（抜粋版）

PCCOMは，柔軟性とセキュリティを兼ね備えた通信グループの構築を可能とするFPN（Flexible Private Network）※を実現するためのネットワークアーキテクチャGSCIP（Grouping for Secure Communication for Internet Protocol）※のプロトコル群のひとつとして機能している．GSCIPを実装するにあたり，基本設計書を作成したので付録として添付する．

※ FPN，GSCIPの詳細は http://www.wata-lab.meijo-u.ac.jp/research/fpn1.html を参照

GSCIP 基本設計書（抜粋版）

著者：増田 真也 （マスダ シンヤ） 名城大学大学院理工学研究科情報科学専攻
監修：渡邊 晃 （ワタナベ アキラ）名城大学理工学部情報工学科 教授

最終更新日：2005 年 10 月 30 日

1. はじめに

本書は FPN を実現するためのネットワークアーキテクチャ GSCIP（ジースキップ；Grouping for Secure Communication for Internet Protocol）の基本設計書である．

GSCIP は DPRP（Dynamic Process Resolution Protocol），Mobile PPC（Mobile Peer-to-Peer Communication），Mobile NPC（Mobile Network-to-Peer Communication），NATF（NAT Free protocol），PCCOM（Practical Cipher COMmunication），SPAIC（Secure Protocol for Authentication with IC Card）の 6 つのプロトコルから構成され，GSCIP のプロトコルスタックを GPACK(GSCIP PACKage)と呼ぶ．GSCIP の構成を図 1-1 に示す．

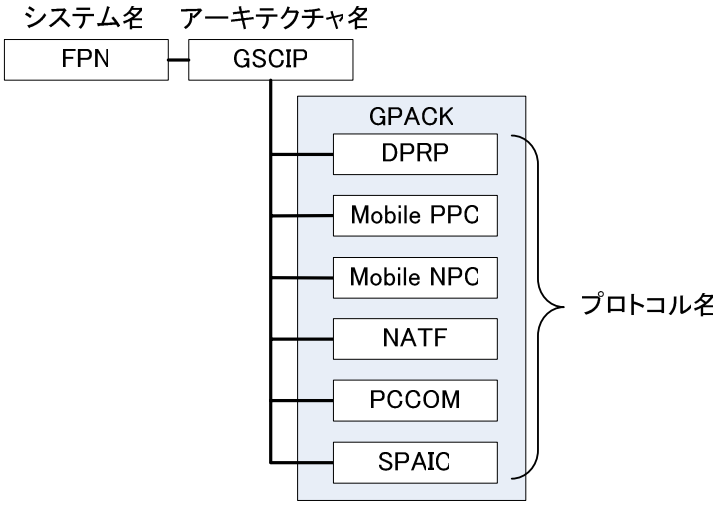


図 1-1 GSCIP の構成

また，GSCIP を管理する装置を MS（Management Server），GPACK の動作処理を規定したテーブルを GPIT（GSCIP Process Information Table）と呼ぶ．GSCIP のドキュメント体系を図 1-2 に，一覧表を表 1-1 に記す．

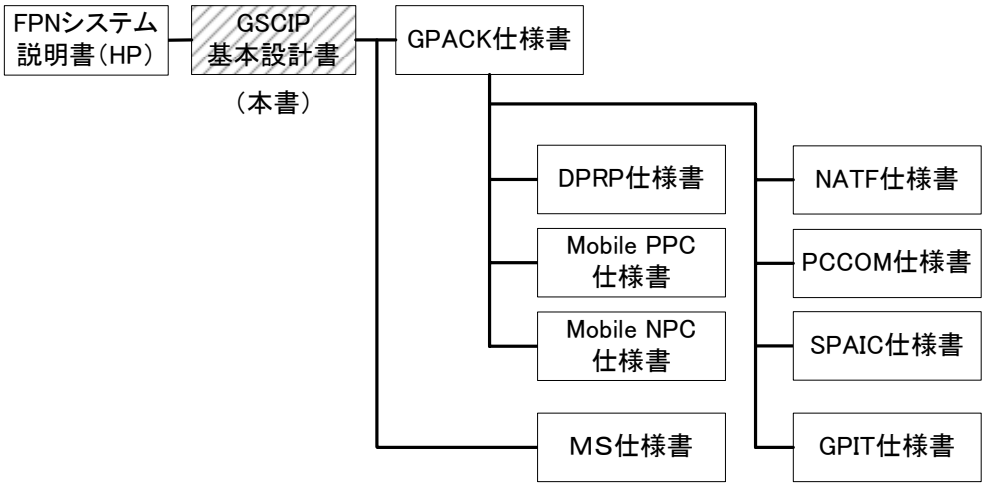


図 1-2　GSCIP のドキュメント体系

表 1-1　ドキュメント一覧

ドキュメント名	内容
FPN システム説明書	FPN の概念について記した説明書 （HP；http://www.wata-lab.meijo-u.ac.jp/research/fpn1.html）
GPACK 仕様書	GSCIP のプロトコルスタック GPACK の仕様書
DPRP 仕様書	事前交渉プロトコル DPRP の仕様書
Mobile PPC 仕様書	移動体通信プロトコル Mobile PPC の仕様書
Mobile NPC 仕様書	ネットワーク単位の移動透過性を実現する Mobile PPC の仕様書
NATF 仕様書	アドレス空間の違いを意識しない NATF の仕様書
PCCOM 仕様書	実用暗号通信プロトコル PCCOM の仕様書
SPAIC 仕様書	セキュア鍵配送プロトコル SPAIC の仕様書
GPIT 仕様書	動作処理情報テーブル GPIT の定義と動作を記した仕様書
MS 仕様書	GSCIP の管理装置の仕様書

GSCIP が提供するシステムは大きく分けて，グルーピングされた端末の柔軟でセキュアな通信を提供する“閉域通信グループ”，通信中に IP アドレスが変化した場合もコネクションを切断することなく通信を継続することができる“移動体通信システム”，グローバルアドレスとプライベートアドレスの違いを意識せずに通信を可能とする“アドレス空間透過システム”の 3 つから成る．GSCIP を実装した装置を GE（GSCIP Element）と呼び，これにより，FPN が想定するロケーションフリーが実現する．

2. システム構成

2.1. 閉域通信グループ

閉域通信グループの構成要素を図 2-1 に示す．閉域通信グループは，FPN の最も基本となる部分である．グルーピングを構築するのは GE で，移動端末 MN（Mobile Node）などの端末自体をグルーピングする GES（GSCIP Element for Software），ルータのサブネット全体をグルーピングする GEN（GSCIP Element for Network），ブリッジ配下のサーバをグルーピングする GEA（GSCIP Element for Adopter）に分類される．GE はグループ鍵 GK（Group Key）を保持しており，同一の GK を持つ GE の集合を通信グループとして定義する．GK の番号とグループの番号は 1 対 1 で対応し，同一グループの通信は GK を用いた暗号化によって保護される．管理装置 MS は各 GE に対して認証を行った後，グループ定義情報およびグループ番号に対応したグループ鍵を配送する．MS は通信グループの定義のみを行い，GE の物理的位置関係は管理しない．各 GE は通信経路上の自己の位置を学習し，通信に必要となる動作処理情報を自動生成する．GES を実装した移動端末は，場所を移動した場合においてもグルーピングの関係が自動的に維持される．

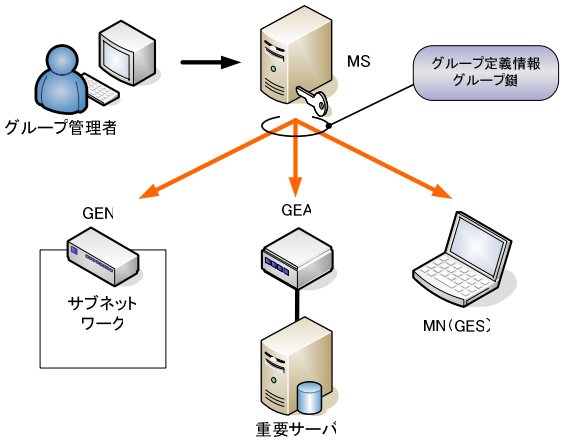


図 2-1　閉域通信グループの構成要素

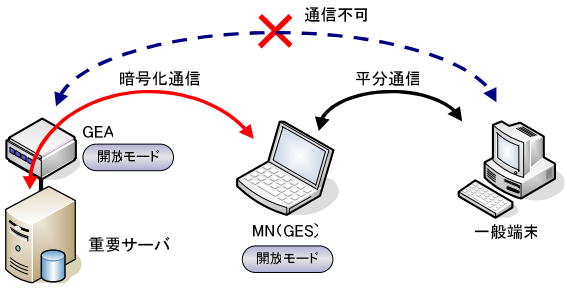


図 2-2　閉域モードと開放モード

GE にはグループ外のメンバとの通信を全く禁止する閉域モード（Closed Mode）と，一般通信を可能とする開放モード（Open Mode）がある（図 2-2）．閉域モード GE は外部からの不正侵入を防ぐのが目的で使用され，サブネットの入り口か，重要なサーバの手前に設置する．一方，開放モード GE は一般にクライアントに適用し，重要なサーバへのアクセスが可能であると同時に，一般サーバへのアクセスが可能である．また開放モードは，閉域モード内のサブネットに存在するユーザが，外部ユーザとの通信を可能とするためのプロキシサーバにも適用される．

グループ構成単位は，個人単位（権利者単位）とサブネットワーク単位（部門単位）がある（図 2-3）．個人単位の場合はきめ細かい定義が可能であり，GES や GEA で実現できる．サブネット単位の場合は管理単位が大きいので管理負荷を軽減できるという利点があり GEN で実現できる．GES，GEA，GEN は混在することが可能である．企業で言えば，部門単位の通信グループが GEN で構成されているが，部門内の特定メンバは社内横断のプロジェクトに参画したり，役職別にアクセスポリシーを設定したりしており，GES を保持して個別に別通信グループにも帰属しているようなケースが想定できる．通信グループとは，このように同一の仕事をするメンバによるグループとほぼ対応させることができる．

動作処理情報（暗号化/復号，透過中継，廃棄）の動的な生成は DPRP 仕様書，通信パケットの暗号化は PCCOM 仕様書，動作処理情報テーブル GPIT の仕様は GPIT 仕様書，MS-GE 間の認証は SPAIC 仕様書，MS の仕様は MS 仕様書を参照されたい．

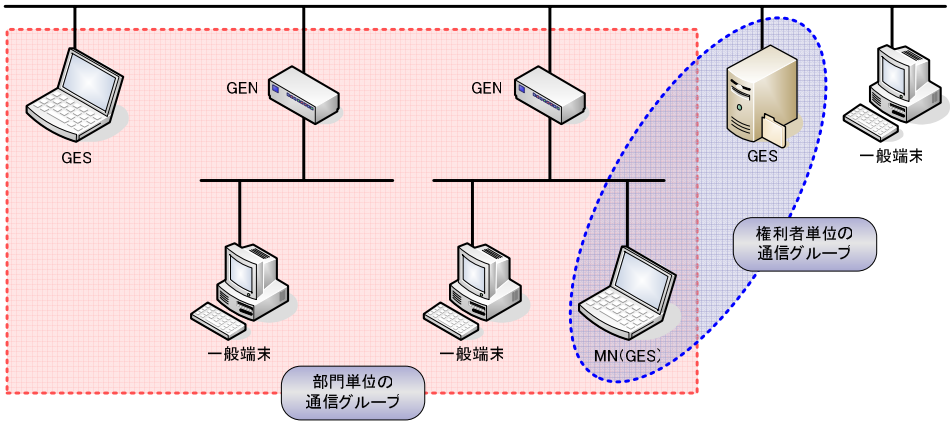


図 2-3　グループ構成単位

2.2. 移動体通信システム

移動体通信システムの構成要素を図 2-4 に示す．移動体通信システムは，移動ノード MN，ネットワークモビリティを提供する MPR（Mobile PPC Router），DDNS（Dynamic DNS）から構成される．MN は GES，MPR は GEN の機能を包含する．それぞれの詳細は Mobile PPC 仕様書，Mobile NPC 仕様書を参照されたい．DDNS は初期 IP アドレスの解決（通信開始時のアドレス解決）に用いられる．通信中に IP アドレスが変化した場合は MN，MPR 間で相互に情報交換を行い，継続 IP アドレスの解決（コネクションを切断することなく通信を継続する動作）を行う．

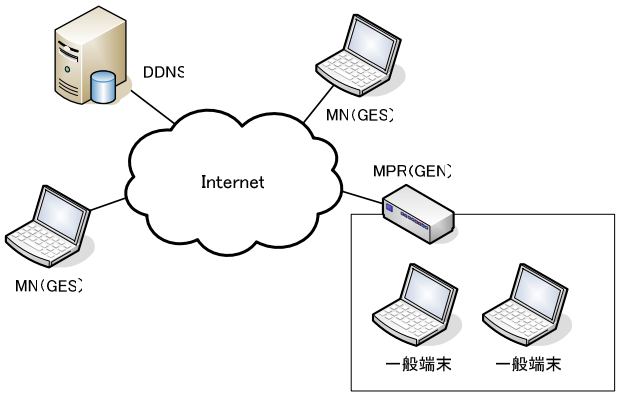


図 2-4　移動体通信システムの構成要素

2.3. アドレス空間透過システム

アドレス空間透過システムの構成要素を図 2-5 に示す．システムは，NATF ボックス，NATF 端末，DDNS から構成される．NATF ボックス，NATF 端末は GES の機能を包含する．NATF の機能により，グローバルアドレスとプライベートアドレスの違いを意識せずに通信することができる．また，グローバルアドレス空間を跨るプライベートアドレス空間端末同士の通信を可能とする（プライベートアドレス空間同士でアドレスの重複があってもよい）．詳細は NATF 仕様書を参照されたい．

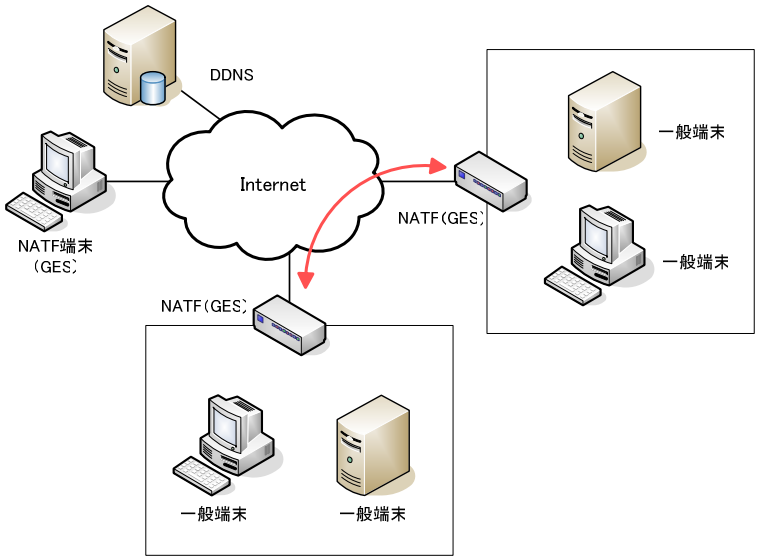


図 2-5　アドレス空間透過システムの構成要素

3. システムの機能・プロトコル

GES，GEA，GEN，MS が保持する機能・プロトコルは，表 2-1 のとおりである．

表 3-1　各装置の機能・プロトコル

装置	機能・プロトコル
GES/GEA/GEN	プロトコル DPRP Mobile PPC Mobile NPC NATF PCCOM SPAIC（SPAIC Client，SPAIC GEN/GEA 用）
MS	機能 ユーザ管理 グループ管理 グループ鍵生成 ヘルスチェック プロトコル SPAIC（SPAIC Server）

3.1. GES/GEA/GEN のプロトコル概要

- DPRP
  GE の動作処理情報をシステム構成に応じて自動生成する．
- Mobile PPC
  アドレス変換機能を保持させ，通信中に IP アドレスが変化した場合もコネクションを切断することなく通信を継続する．
- Mobile NPC
  Mobile PPC と NAT を連動させることで，ネットワーク単位の移動透過性を実現する（GEN）．
- PCCOM
  グループ鍵を用いてデータを暗号化/復号する．このとき，パケットの完全性保証の処理も行う．
- SPAIC（SPAIC Client）
  グループ鍵や各種ユーザ情報の取得する際に，MS と GE 間での確実な認証を行う．MS との連動は IC カード用アプリケーション（GES），MS 用デーモン（GEA/GEN）で行われ，その際の認証に SPAIC が動作する．

3.2. MS の機能・プロトコル概要

- ユーザ管理
  ユーザ名を管理する．
- グループ管理
  グループ番号を管理し，各ユーザがどのグループに所属しているかを管理する．
- グループ鍵生成
  グルーピングに用いる共通暗号鍵を生成する．
- SPAIC（SPAIC Server）
  ユーザ情報に基づいたグループ鍵や各種情報を配送する際に，MS と GE 間での確実な認証を行う．

4. まとめ

FPN を実現するためのセキュリティアーキテクチャ GSCIP の基本設計を記した．本設計書では，GSCIP の基本要素しか規定しておらず，実際にはその応用として，プライベートアドレス空間とグローバルアドレス空間の移動透過性の実現や，異なるプライベートアドレス空間同士の通信を実現する CIPA（Communication between terminals in Independent Private Address areas）などを提案・実装している．これらにつては，それぞれの関連文献を参照されたい．

C　MS 仕様書（抜粋版）

GSCIP を運用するには，通信グループやユーザ，鍵などを管理する装置 MS（Management Server）が必要である．MS を実装するにあたり，仕様書を作成したので付録として添付する．

MS 仕様書（抜粋版）

著者：増田 真也 （マスダ シンヤ） 名城大学大学院理工学研究科情報科学専攻
監修：渡邊 晃 （ワタナベ アキラ）名城大学理工学部情報工学科 教授

最終更新日：2005 年 1 月 19 日

1. はじめに

管理装置 MS（Management Server）は，FPN（Flexible Private Network）を実現するためのセキュア通信アーキテクチャ GSCIP（Grouping for Secure Communication for Internet Protocol ; ジースキップ）のシステムを管理する装置である．

MS はユーザやグループの管理，GE の管理，グループ共通鍵・グループ鍵の管理と配送などを行う（本仕様では閉域通信グループのみを管理対象とし，アドレス空間透過性を実現する NATF，移動透過性を実現する MPPC は考慮していない）．

本仕様書では，MS の機能とシステム構成および設計について述べる．FPN の概念については「FPN システム説明書」を，GSCIP の基本動作については「GSCIP 基本設計書」を，MS の重要情報を安全に配送するプロトコル SPAIC については「SPAIC 仕様書」を，GPIT の定義と動作については「GPIT 仕様書」をそれぞれ参照すること．本仕様書に関連するドキュメントの一覧を表 1-1 に記す．

表 1-1 関連ドキュメント

ドキュメント名	内容
FPN システム説明書（Web）	FPN の概念について記した説明書 （http://www.wata-lab.meijo-u.ac.jp/research/fpn1.html）
GSCIP 基本設計書	FPN を実現するためのアーキテクチャ GSCIP の基本設計書
GPACK Main Module 仕様書	GSCIP を実現するモジュール群 GPACK の仕様書
SPAIC 仕様書	MS の重要情報を安全に配送するプロトコル SPAIC の仕様書
GPIT 仕様書	動作処理情報テーブル GPIT の定義と動作を記した仕様書

2. MS

2.1. システム構成

図 2-1 は GSCIP のシステムにおいて，MS の動作に関わる装置のシステム構成である．MS は Web ベースアプリケーションとして機能し，管理者端末から Web ブラウザを通じて MS を操作する．GEN，GEA に配送するグループやグループ鍵などの情報は，Web ベースアプリケーションと各 GE で動作する MS 用デーモン msd でやりとりする．GES にはユーザ情報を読み込む IC カードリーダが搭載されており，カード内のユーザ情報を用いて MS からグループやグループ鍵などの情報を取得する．IC カード用アプリケーションはその動作を担う．

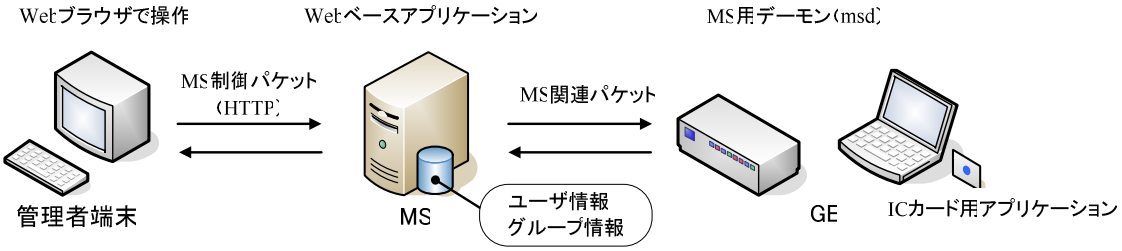


図 2-1　システム構成

2.2. 機能

2.2.1.　MS

- ✧ IC カード生成
  公開鍵ペア生成，IC カードへの書き込み（GES 用）
- ✧ 初期情報の設定
  公開鍵ペア生成，GEN, GEA へ秘密鍵の埋め込み（オフライン）
- ✧ ユーザ登録
  加入するユーザ ID を登録，ホスト名の設定（GEN/GEA のみ），GEN,GEA,GES の種別，開放/閉域の指定
- ✧ グループ登録
  グループ番号とグループ名を登録
- ✧ グループ定義
  ユーザ ID とグループを対応づける
  グループ別とユーザ別に登録が可能
- ✧ 初期情報の配送
  GES の IC によるカードログイン時または GEN/GEA の立上げ時に出される要求をトリガとし，初期情報（グループ番号，閉域/開放，グループ鍵）を配送
  または，MS 側から管理者の指示で配送
- ✧ グループ鍵（CK 含む）の配送指示/履歴表示
  オンデマンドの指示で新しいグループ鍵を生成して配送（GEN/GEA のみ）
  定期配送のための時刻指定（GEN/GEA のみ）
  配送履歴の表示
- ✧ ログ表示
  MS の動作記録をログに出力する．動作の種別は，ユーザ登録，グループ登録，グループ定義，初期情報配送，グループ鍵配送　がある．
- ✧ 状態確認とその表示
  状態確認パケットをオンライン GE に送信しその応答パケットより，現在システムに参加している GE とグループを表示，鍵バージョンも表示
  現在システムに参加している GE とグループを表示，鍵バージョンも表示
  オンライン GE のヘルスチェック，オンライン GE とそのグループの関係を一覧表示
  GES からログアウト情報を受信した場合，状態をオフラインに変更

2.2.2. msd

- ✧ 初期情報の要求
  GEN/GEA 立上げ（デーモン起動）時に，初期情報を MS に要求
- ✧ 初期情報の受信
  MS から配送される初期情報または MS 側から管理者の指示で配送される初期情報を受信し，システムコールで設定を反映
- ✧ グループ鍵の受信
  MS から送られるグループ鍵を受信し，システムコールで反映（GEN,GEA）
- ✧ 状態確認応答
  MS から送られる状態確認パケットを受信し，応答パケットとして GE 情報，グループ，鍵バージョンを送信

2.2.3. IC カード用アプリケーション

- ✧ 初期情報の要求
  IC カードによるログイン時に，初期情報を MS に要求
- ✧ 初期情報の受信
  MS から配送される初期情報を受信し，システムコールで設定を反映
- ✧ 状態確認応答
  MS から送られる状態確認パケットを受信し，応答パケットとして GE 情報，グループ，鍵バージョンを送信
- ✧ ログアウト情報の送信
  ユーザがログアウトしたら MS へログアウト情報を送信する

2.3. MS 用データベース

MS にはユーザ情報やグループ情報を記録したデータベース（以下，DB）を保持している．DB の各テーブル内容を以下に示す．なお，フィールドの下線は主キーを意味する.

2.3.1. ユーザ情報（tbl_UserInfo）

表 3-1 ユーザ情報

UserID	UserName	HostName	GEType	Mode	Enable	State	Checking
********* (9 桁)	GEN1		1 (GEN)	1(OP)	1（Enable）	1（On）	1（Checking）
********	GEA1		2 (GEA)	2 (CL)	0（Disable）	2（Off）	2（Reply）
********	user1		3 (GES)	1 (OP)	1（Enable）	3（Maintenance）	1（Checking）
********	user2		3 (GES)	2 (CL)	1（Enable）	9（Error）	1（Checking）

2.3.2. グループ情報（tbl_GroupInfo）

表 3-2 グループ情報

GroupNumber	GroupName	Enable	KeyVersion	GK
********	Group1	1（Enable）	***（3 桁）	********
********	Group2	0（Disable）	***	********

2.3.3. 所属グループ情報（tbl_BelongGroupInfo）

表 3-3 所属グループ情報

UserID	GroupNumber
********	********
********	********

2.3.4. 公開鍵管理(tbl_PKManagement)

表 3-4 公開鍵管理

PKNumber	KeyVersion	PK
********	********	**********
********	********	**********

2.3.5. 設定(tbl_MSConf)

表 3-5 設定

GKLen	PKLen	Periodic	Check Interval
可変 ※1	可変 ※2	00:00:00	1~255（秒）

※1 1 :64, 2:128, 3:256, 4:512（単位：ビット）※2 1 :256, 2:512, 3:1024, 4:2048（単位：ビット）

2.3.6. ログ(tbl_Log)

表 3-6 ログ

Type	RegDate	DistDate	Process	KeyVersion	UserID	GroupNumber
1（ユーザ登録）	****		1（追加）		****	
2（グループ登録）	****		2（更新）			****
3（グループ定義）	****		3（削除）		****	****
4（鍵更新）	****		2（更新）	********		****
5（初期情報配送）		****		********	****	****
6（グループ鍵配送）		****		********	****	****

2.4. 通信内容

図 2-2 に MS-GE 間の通信内容を示す（通信内容の種別を図示しているだけで，シーケンスではない）．図中の N，A，S はそれぞれ GEN，GEA，GES を指す．

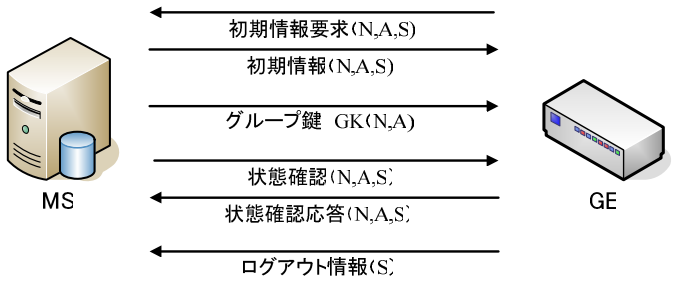


図 2-2 通信内容

2.5. 動作

管理者端末，MS，GE の間でやりとりされる動作（処理体系）を以下にまとめる．なお，各動作の図で用いられている記号の意味は図 2-3 の通りである．

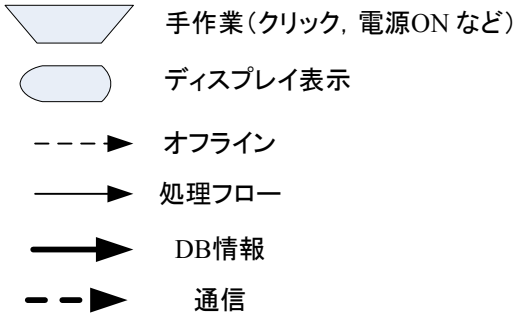


図 2-3 記号

2.5.1. IC カード生成（GES）

MS が，データベース（以下，DB）の設定テーブルから公開鍵長（PKLen）を読み込み，それを元に公開鍵ペアを生成する．公開鍵は MS に保存し，秘密鍵は IC カードへ書き込む．

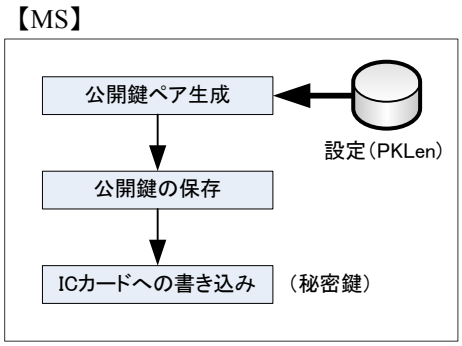


図 2-4 IC カード生成

2.5.2. 初期情報の設定

MS が，DB の設定テーブルから公開鍵長（PKLen）を読み込み，それを元に公開鍵ペアを生成する．公開鍵は MS に保存し，秘密鍵は GEN，GEA にオフラインで埋め込む．

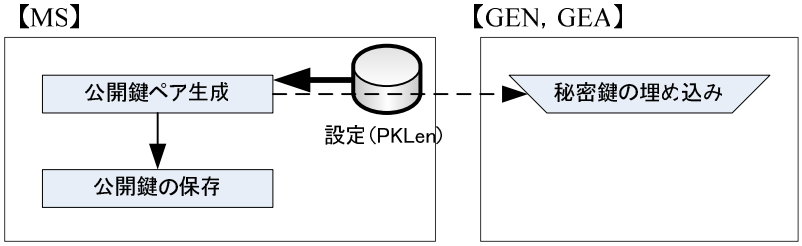


図 2-5 初期情報の設定

2.5.3. ユーザ登録

管理者端末のユーザ登録画面より，加入するユーザ ID を登録，ホスト名の設定（GEN/GEA のみ），GEN,GEA,GES の種別，開放/閉域を指定し，登録内容を DB のユーザ情報テーブルに書き込む．結果をユーザリストとして管理者端末に表示する．ユーザ情報を修正する場合は，DB のユーザ情報テーブルの内容を得た管理者端末のユーザ登録画面より，修正・削除の指示をし，変更内容を DB のユーザ情報テーブルに書き込む．登録履歴は DB のログテーブルに記録する．

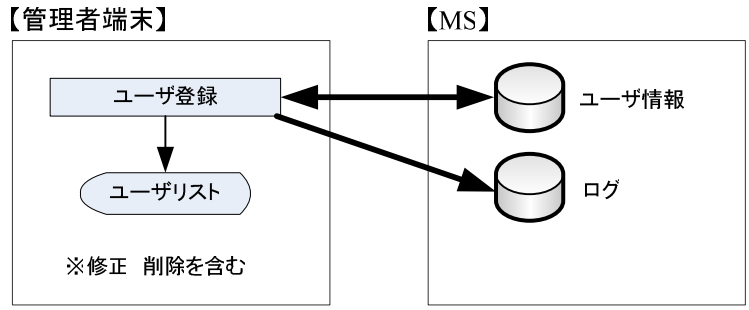


図 2-6 ユーザ登録

2.5.4. グループ登録

管理者端末のグループ登録画面より，グループ番号とグループ名を設定して登録内容を DB のグループ情報テーブルに書き込む．次に，グループに対応する共通暗号鍵を MS にて生成して保存し，その情報を DB のグループ情報テーブルに書き込む．登録履歴は DB のログテーブルに記録する．

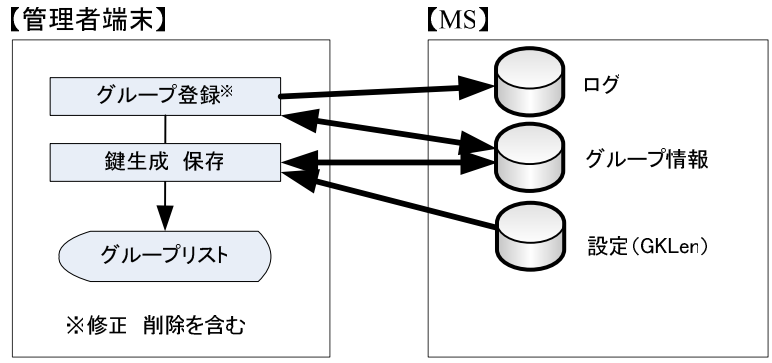


図 2-7 グループ登録

2.5.5. グループ定義

管理者端末のグループ定義画面（ユーザ別とグループ別がある）より，DB のユーザ情報テーブルとグループ情報テーブルからユーザ ID・ユーザ名とグループ番号・グループ名を読み込み，ユーザ ID とグループを対応づけ，内容を DB のグループ定義テーブルに保存する．グループに対してユーザを登録する方法とユーザに対してグループを登録する方法の２つがある. 定義履歴は DB のログテーブルに記録する．

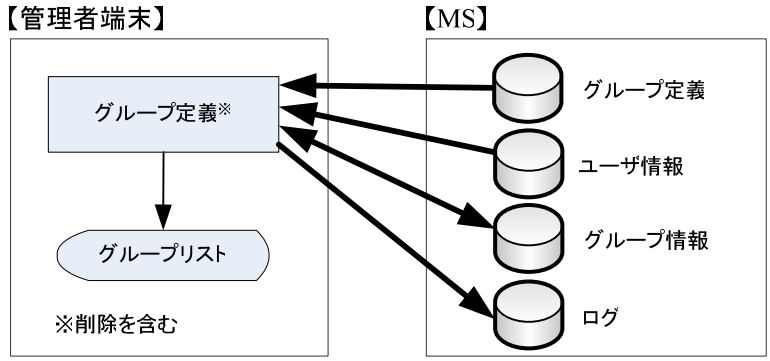


図 2-8 グループ定義

2.5.6. 初期情報の配送

管理者端末の配送指示により，MS にて DB のユーザ情報テーブル，グループ情報テーブル，グループ定義テーブルを元にグループ番号，開放/閉域，GK，を全オンライン GEN,GEA に対して配送する．GE では配送された初期情報をシステムコールで反映させる．

また，GEN，GEA の電源 ON（デーモン起動）時あるいは GES の IC カードを用いたログイン時には，MS に初期情報を要求し，要求を受けた MS は DB のユーザ情報テーブルに要求元の GE がオンラインであることを記録し，要求元が GES の場合はユーザ情報テーブルにホスト名を記録する．次に，DB のユーザ情報テーブル，グループ情報テーブル，グループ定義テーブルを元にグループ番号，開放/閉域，GK，を要求元に配送する．GE では配送された初期情報をシステムコールで反映させる．

配送履歴は DB のログテーブルに記録する．

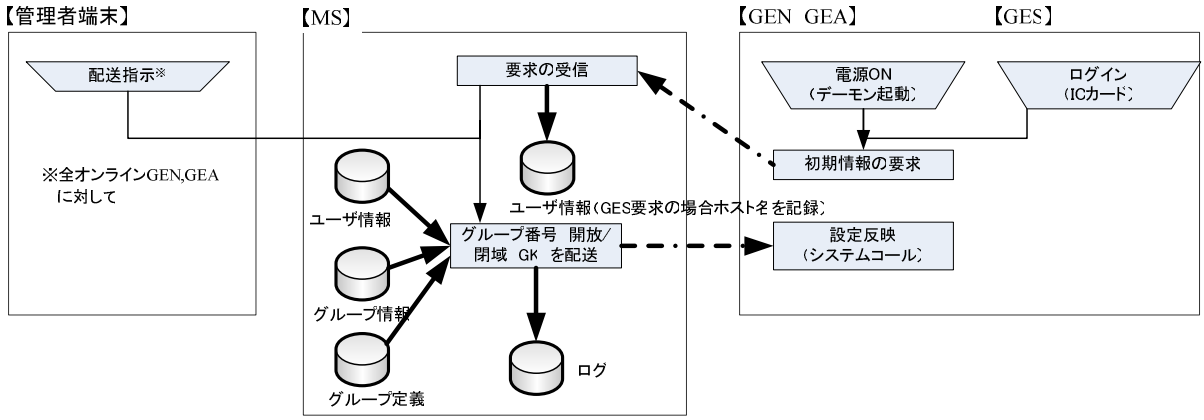


図 2-9 初期情報の配送

2.5.7. グループ鍵の配送/履歴表示

管理者端末の配送指示により，MS にて DB のユーザ情報テーブル，グループ情報テーブル，グループ定義テーブルを元に GK または CK を全オンライン GEN,GEA に対して配送する．GE では配送された鍵情報をシステムコールで反映させる．

また，MS では定期的に新鍵を生成し，全オンライン GE に対して鍵の配送を行う．定期配送の間隔は DB の設定テーブルより読み込む．新鍵は DB の設定テーブルからグループ鍵長（GKLen）を読み込み，それを元に生成する．GE では配送された鍵情報をシステムコールで反映させる．

配送履歴は DB のログテーブルに記録する．

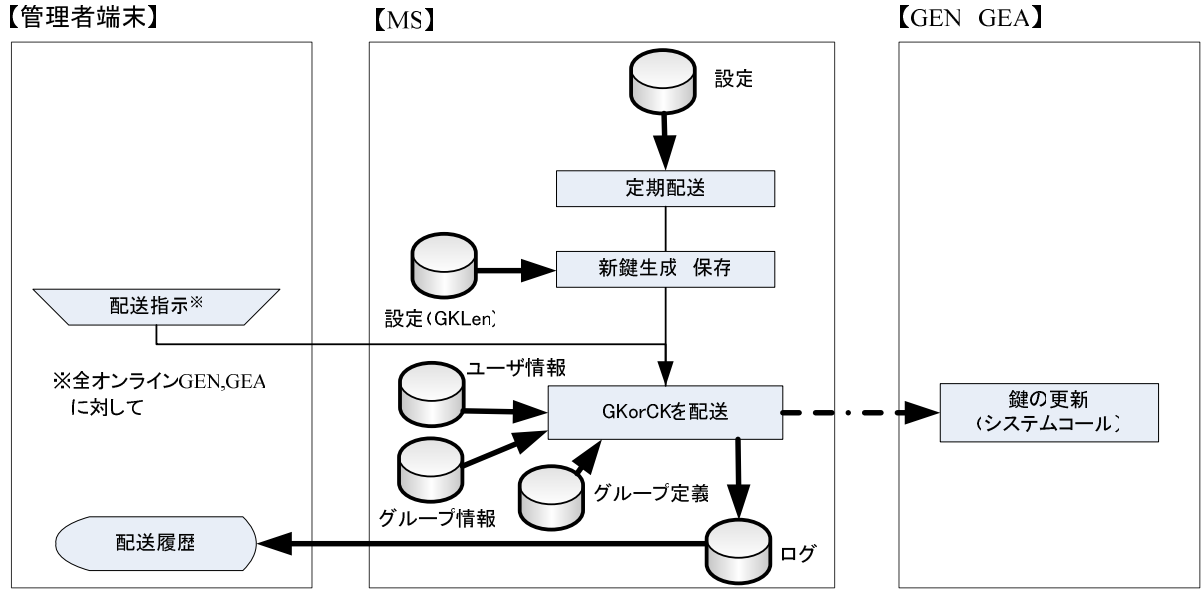


図 2-10 グループ鍵の配送/履歴表示

2.5.8. ログ表示

管理者端末のログ表示画面にて，DB のログテーブルからログを読み込み表示する．

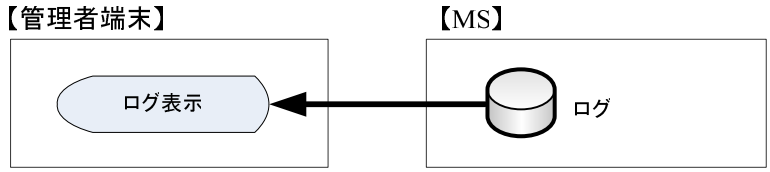


図 2-11 ログ表示

2.5.9. 状態表示

管理者端末が状態表示指示を出すと，DB のユーザ情報テーブル，グループ情報テーブル，グループ定義テーブルを元に，管理者端末の画面に各 GE の状態を表示する．

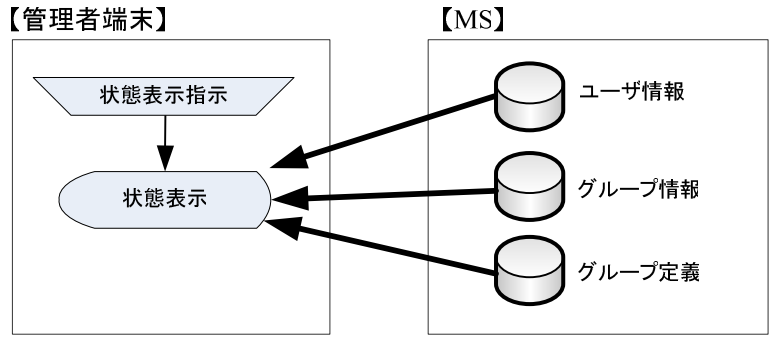


図 2-12 状態表示

2.5.10. ログアウト情報伝達

GES はログアウトを行うと，MS にその情報を伝達する．情報を受けた MS は DB の状態管理テーブルに伝達元の GES がオフラインになったことを記録し，ユーザ情報テーブルに記録されたホスト名を消去する．

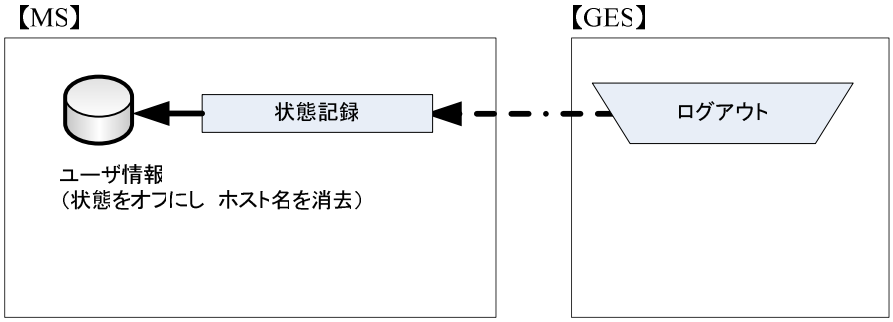


図 2-13 ログアウト情報伝達

2.5.11. ヘルスチェック

MS は全オンライン GE に対して定期的にヘルスチェック（状態管理処理）として状態確認パケットを送信する．状態管理パケットを受信した GE は状態確認応答パケットを MS に送信する．状態確認応答パケットを受信した MS は送信元の GE がオンラインであることを DB のユーザ情報テーブルに記録する．一定時間経過しても GE から応答が無い場合は，オフラインとして記録する．

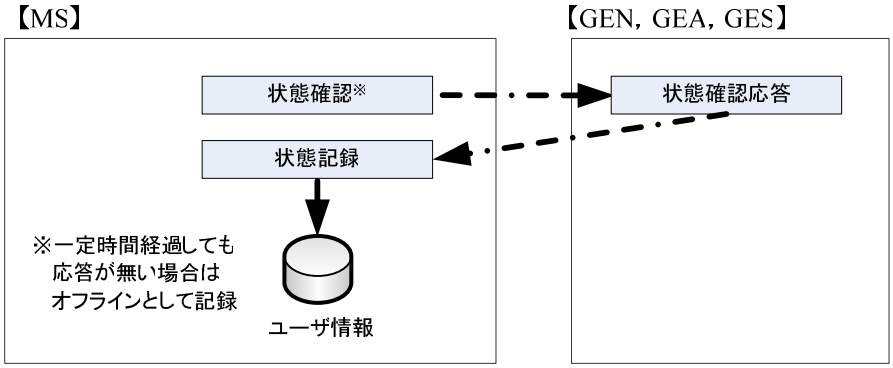


図 2-14 ヘルスチェック

3. パケットフォーマット

MS 関連の処理でやりとりするパケットは UDP をベースに定義されている．パケットの構造を図 3-1 に示す．UDP のポート番号は **12345 番**（仮）とし，この番号のパケットには UDP ペイロードに MS ヘッダと MS データが存在することになる．

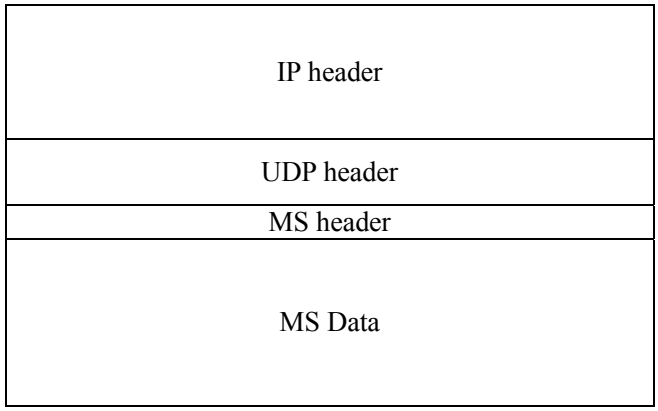


図 3-1 MS 関連パケットの構造

3.1. MS ヘッダ

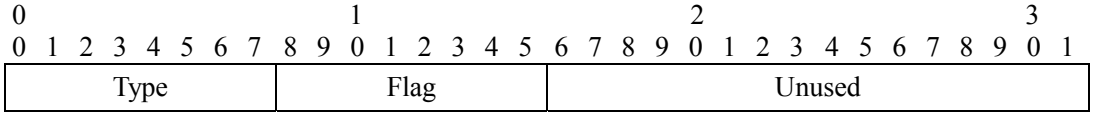


図 3-2 MS ヘッダフォーマット

表 3-1 MS ヘッダフィールド

フィールド	サイズ	値
Type	1	定義（表 3-2）
Flag	1	未定義
Unused	2	未使用

表 3-2 Type の定義

名前	値	説明
MSD_INITINFO	1	初期情報
MS_INITIINFO_REQ	2	初期情報要求
MSD_STATE	3	状態確認
MS_STATE_ACK	4	状態確認応答
MSD_GKDIST	5	グループ鍵配送
MS_LOGOUT	6	ログアウト情報
NS_ERROR	9	エラー処理

3.2. 初期情報

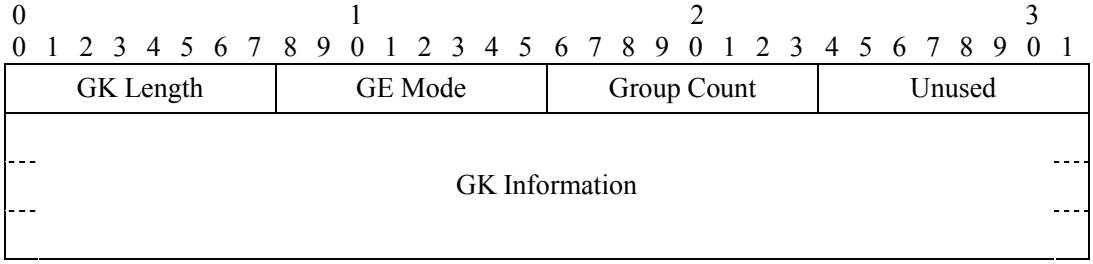


図 3-3 初期情報フォーマット

表 3-3 初期情報フィールド

フィールド	サイズ	値
GK Length	1	GK の鍵長
Mode	1	Open（１）: 開放，Close（２）: 閉域
Group Count	1	グループ数（その数だけ GK 情報がある）
Unused	1	未使用
GK Information	可変長	GK 情報

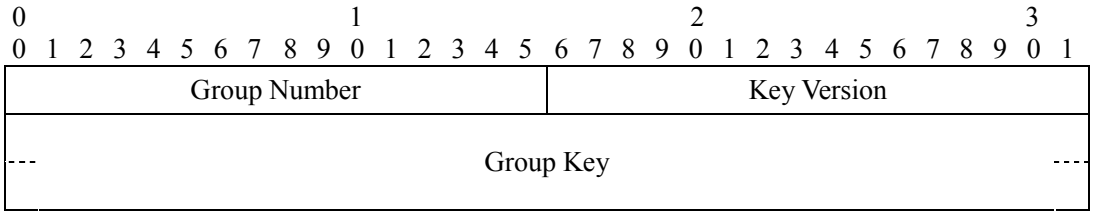


図 3-4 GK 情報フォーマット

表 3-4 GK 情報フィールド

フィールド	サイズ	値
Group Number	2	グループ番号
Unused	2	未使用
Group Key	可変長	グループ鍵（GK および CK）サイズは GK Length

3.3. 初期情報要求

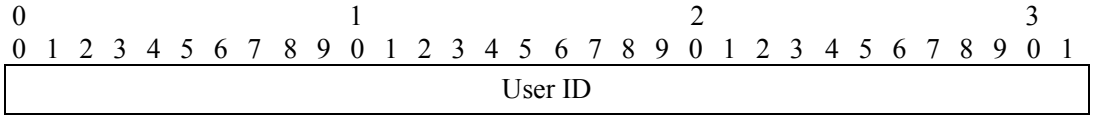


図 3-5 初期情報要求フォーマット

表 3-5 初期情報要求フィールド

フィールド	サイズ	値
User ID	4	ユーザ ID

3.4. グループ鍵配送

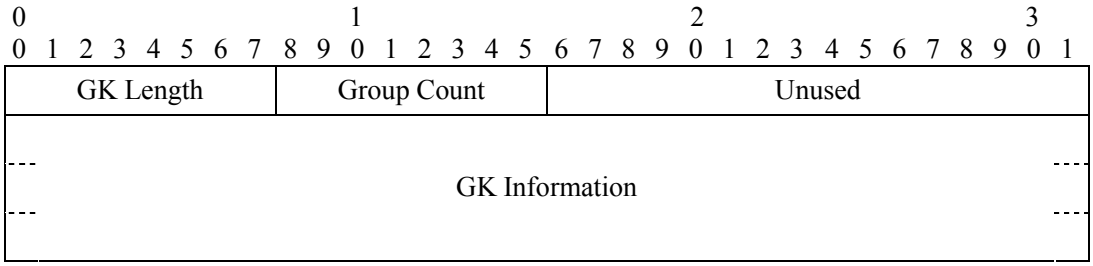


図 3-6 グループ鍵配送フォーマット

表 3-6 グループ鍵配送フィールド

フィールド	サイズ	値
GK Length	1	GK の鍵長
Group Count	1	グループ数（その数だけ GK 情報がある）
Unused	2	未使用
GK Information	可変長	GK 情報（図 3-4，表 3-3）

3.5. 状態確認

None：
オンライン GE に対して状態確認パケットを送信. 状態確認パケットは MS ヘッダの Type で判別.

3.6. 状態確認応答

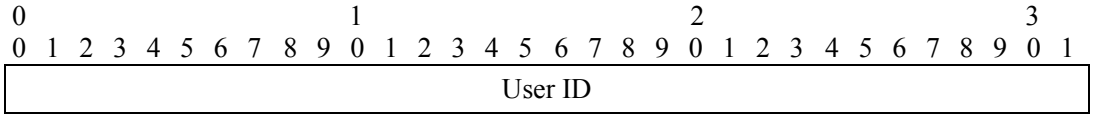


図 3-7 状態確認応答フォーマット

表 3-7 状態確認応答フィールド

フィールド	サイズ	値
User ID	4	ユーザ ID

3.7. ログアウト情報

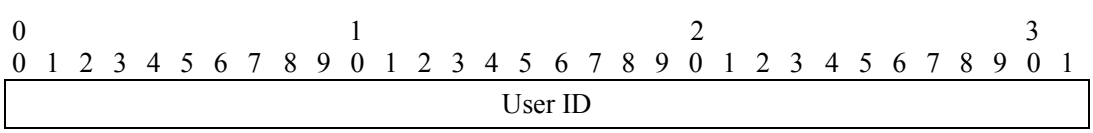


図 3-8 ログアウト情報フォーマット

表 3-8 ログアウト情報フィールド

フィールド	サイズ	値
User ID	4	ユーザ ID