多段構成ネットワークにおける鍵配送方式の一検討

保母　雅敏　渡邊　晃

イントラネット内で安全な通信を行うための技術として，FPN(Flexible Private Networks)を構築する研究が行われている．FPN では，一定の条件でグループ化された暗号装置(EE)間において，共通のグループ鍵を用いて暗号通信を行う．EE では暗号通信の他に，不正なパケットの通過を防止する役割がある．また，グループ鍵は管理装置(MS)から EE へ配送される．本論文では，従来の鍵配送において検討されていなかった，通信経路上に第三の暗号装置(中間 EE)が存在する場合におけるパケットの認証について検討を行い，中間 EE において確実な認証によってパケットの中継可否を決定できるセキュア鍵配送方式 SKDP(Secure Key Distribution Protocol)を提案する．SKDP では PKI 技術を利用し，中間 EE においてディジタル署名の認証を行うことによって鍵配送パケットの確実な認証を行うことを可能とした．

Research of a Key Distribution Method for Vertical Networks

Masatoshi HOBO, Akira WATANABE

One way to communicate securely in Intranet is a study of Flexible Private Networks (FPN). In FPN, grouped devices which make FPN called Encryption Element (EE) communicate using a common group key. Furthermore EEs prevent from wrong packet. Group key is distributed to EE from Management Server (MS). However, when group key are distributed, there are EEs in communication route. In this case, key distribution packets pass midway EE without certification. In this paper, we suggest “Secure Key Distribution Protocol (SKDP)”. SKDP is possible to certify key distribution packet at midway EE.

1. はじめに

ネットワーク技術の発展に伴い，企業などにおいてイントラネットの構築が盛んに行われるようになっている．ネットワークを介してファイルの管理や電子文書のやり取りをすることが可能になり，その利便性は飛躍的に向上している．しかし，イントラネットにおいてもインターネットと同様セキュリティに関する問題が指摘されている．多くのイントラネット環境ではファイアウォールを介してインターネットと繋がっていることが多いため，クラッカーなどによる外部からイントラネットへの不正アクセスの対処や，企業支社との通信といったインターネットを介して他のイントラネットと通信する際の安全確保といった問題が挙げられている．また，イントラネット内部における不正アクセスも年々深刻な問題となってきている．VPN(Virtual Private Network)技術の登場により，イントラネット同士を結ぶ場合などにおいて，インターネット上の通信の安全を確保することが可能となった．しかし，VPN 技術だけではイントラネット内の不正アクセスに対して十分な安全を確保することは困難である．このことから，イントラネット内で安全な通信を行うための技術として，閉域通信グループ(CCGI : Closed Communication Group of Intra-networks)を構築する研究[1]-[3]が行われている．

CCGI を構築するための方法には，VPN 技術の標準である IPSec[4]-[6]を用いる方法が考えられている．IPSec は強力なセキュリティを備えているが，通信経路に対して暗号鍵を割り当てる方式であるため，CCGI 構成要素が多くなると使用される暗号鍵の数が増大して管理が煩雑になる，トンネルモードとトランスポートモードが混在するなどといった課題がある．こ

の課題を解決するための方法の一つとしてFPN(Flexible Private Network)を構築する研究が行われている．FPN では端末の移動や構成の変更，通信経路上に 3 台以上の暗号装置(EE : Encryption Element)が存在するような多段構成ネットワークに対しても柔軟なシステムを構築することが可能である．この方式では，一定の条件で作られた通信グループと，データを暗号化するための共通鍵を一対一に対応させる方式が提案されている．通信グループに対して割り当てられた共通鍵(グループ鍵)を使用して暗号通信を行うため，IPSec ほどの強力なセキュリティではないが，ユーザの管理が容易であるという利点がある．

グループ鍵は鍵管理装置(MS：Management Server)によって管理され，各 EE の要求に応じて MS から配送される．ネットワークの構成によっては，MS から対象の EE(終端 EE)へグループ鍵を配送する際に，パケット通過の認証を必要とする第三の暗号装置(中間 EE)を通過しなければならない場合があり，従来はこの部分において十分な認証が行われていなかった．従来は中間 EE において認証を行うことが考慮されていなかったため，中間 EE では MS と終端 EE を認証するための情報を所持しておらず，鍵配送パケットであれば無条件で通過してしまうという課題があった．

本論文では，グループ鍵を MS から各 EE に配送するにあたり，通信経路上に中間 EE が存在していても，認証によってパケットの通過の可否を決定できるセキュア鍵配送プロトコル(SKDP ：Secure Key Distribution Protocol)を提案する．SKDP では PKI(Public Key Infrastructure)技術で利用されている公開鍵暗号を用いたディジタル署名を用いて中間 EE の認証を行う．PKI では End-to-End においてディジタル署名の検証を行宇事が想定されているが，本提案では，中間 EE においてもディジタル署名を検証することにより，パケットの正当性を判定し，パケットの通過を決定する．終端 EE から MS へのパケットを送信する際に，MS からの認証を得た終端 EE の公開鍵を認証情報として付加することにより，中間 EE は終端 EE の公開鍵を取得し，これを利用してディジタル署名の検証を行うことが可能となる．これによりデータの正当性が認められた場合，対象のパケットは MS が認証した正規の EE が生成したものであるとしてパケットを中継する．

以下 2 章では，想定されるシステムと，従来使用されていた鍵配送方式を挙げ，その問題点を整理する．3 章では SKDP の詳細を述べる．4 章では SKDP の有効性について検討する．5 章はむすびである．

2. 従来の鍵配送方式とその課題

FPN で想定されているシステム構成と，従来の鍵配送方式の用件を述べ，その課題について整理する．

2.1 想定されるシステム

FPN で想定されるシステム(図 1)では，暗号装置としてクライアントにソフトウェアとして組み込まれる EES(ソフトウェア型 EE)，ネットワークの直前に置き配下のネットワークを保護する EEN(ネットワーク型 EE)，直下の端末のみを直接保護する EEA(アダプタ型 EE)が存在する．これらの EE は企業内の部署同士などといった一定の条件に基づきグループ化され，同じ通信グループに属している端末とは，この通信グループに割り当てられた共通のグループ鍵を用いて暗号通信を行う．また，ネットワーク中に配置することで不正なパケットの通過を防止する．グループ情報とグループ鍵は MS によって管理され，EE からの鍵配送要求に応じて適切な鍵を配送する．EE はグループ情報を保持していないため，端末の一時的な移動や通信グループの再構成といった場合に

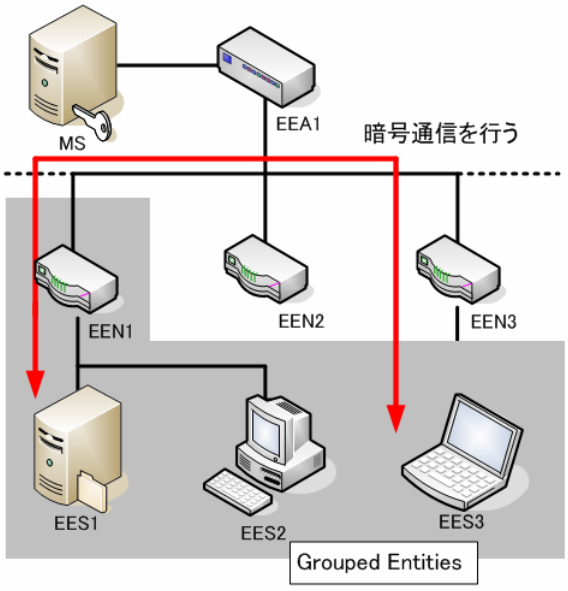

図 1　FPN システムの構成例

Fig.1 Example of FPN system.

おいても容易にグループ情報の変更を行うことが可能である．また，システムの安全性の向上のため，MS は定期的にグループ鍵の更新を行う．グループ鍵の更新は 24 時間程度を想定しているため，通常は常に電源が投入されている状態にある EEN/EEA は電源投入時とグループ鍵更新時に，EES は電源投入時にグループ鍵の配送を行う．

このグループ鍵の配送の際，ネットワーク構成によってはMS と終端EE の経路上に中間EE が存在する場合がある(図 2)．EE には暗号通信を行う機能の他に，不正なパケットの通過を防止する機能があるが，これらの機能が正常に動作するためにはグループ鍵を含めたパラメータが EE に配送されていることが必須となる．EE に暗号通信に必要なパラメータが存在しない場合はパケットが破棄されるため，グループ鍵の配送においてはパケットが中間 EE を通過することが必要である．

2.2 従来方式とその課題

従来の鍵配送方式[7]では，MS と各 EE との間で RSA などの公開鍵暗号ペアを認証秘密情報として用いている．EE はセッションごとに生成される乱数を公開鍵暗号ペアの一方で暗号化し，ユーザ ID などの情報と公開鍵暗号ペアの共通部分を用いてハッシュを生成し，鍵配送要求として MS に送信する．MS はハッシュを検証することで EE を認証し取り出された乱数と公開鍵暗号ペアのもう一方を用いグループ鍵を暗号化し，鍵配送要求と同様にハッシュを生成し鍵配送を行う．EE はハッシュを検証することで MS を認証し，グループ鍵を取得する．この方法では，秘匿された公開鍵暗号ペアを用いているため，End-to-End においてはユーザ認証を行うことが可能である．しかし，経路上に中間 EE が存在する場合，外部に公開できる情報を所持していないため，中間 EE でパケットの認証を行うことが出来ない．

PKI 技術のように公開鍵暗号ペアの一方を外部に公開する方法では，初期情報として各 EE は自身の秘密鍵(Prx)と MS の公開鍵(PuS)，MS は自身の秘密鍵(PrS)と各 EE の公開鍵(Pux)を所持している．EE はセッションごとに生成される乱数 Rx を MS の公開鍵 PuS で暗号化し，ユーザ ID などの情報とともにディジタル署名を生成し，鍵配送要求として MS に送信する．MS は EE の公開鍵 Pux でディジタル署名の検証を行い，自身の秘密鍵 PrS で情報を復号し Rx を得る．この Rx を用いてグループ鍵を暗号化しディジタル署名を付加して EE に送信する．EE は MS の公開鍵 PuS を用いてディジタル署名を検証し，グループ鍵を得る．この方法では公開鍵が外部に公開できる情報であるため，中間 EE は取得した公開鍵を用いることでディジタル署名の検証は可能である．しかし，PKI においても中間 EE での認証は考慮されていない．また，鍵配送時に認証を行うためには全ての EE の公開鍵をユーザ ID と対応づけておかなければならないため，ユーザの追加などが発生した場合の管理負荷が増大してしまう

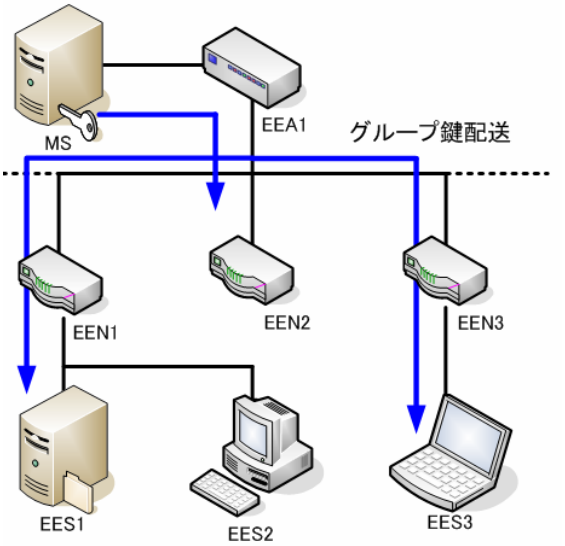

図 2　通信前の鍵配送

Fig.2 Key distribution before communication.

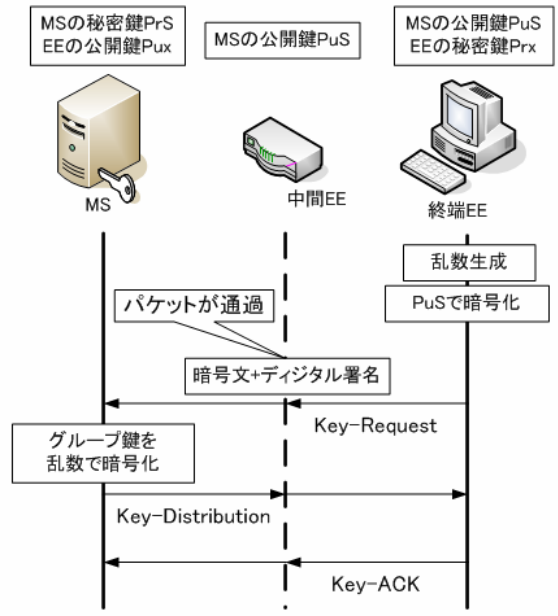

図 3　従来の鍵配送方式の問題点

Fig.3 Problem of conventional key distribution.

という問題がある.

従来はこのように経路上に中間 EE が存在する場合(図 3)の検討が不十分であり，鍵配送のためのパケットは無条件で中間 EE を中継させていた．しかし，どの端末がパケットを送信したかにかかわらずパケットを通過させてしまうため, パケットを偽造することで正常なパケットだけでなく不正なパケットの通過も許してしまうという課題があった. このような中間 EE が存在する環境における鍵配送では，不正なパケットの通過を防ぐため MS が認証した正規の EE が生成したパケットのみを通過させることが必要である.

3. セキュア鍵配送プロトコル SKDP

本章では 2.2 で述べた課題を満たすため，中間 EE が経路上に存在していても認証によってパケットの通過を決定できるセキュア鍵配送方式 SKDP(Secure Key Distribution Protocol)を提案する．以下 3.1 では SKDP の基本原理を示し，3.2 でその動作について述べる.

3.1 中間暗号装置における認証方式

SKDP では PKI を用い，End-to-End だけでなく中間 EE においても認証を行うために，表 1 のような初期情報を保持させる.

従来各 EE には, ユーザ ID(IDx), 秘密鍵(Prx) ，MS の公開鍵(PuS)を初期情報として与えていたが，これに加え，EE の公開鍵を MS の秘密鍵(PrS)で暗号化した認証情報 Eprs[Pux]を新たな初期情報として追加する．MS には従来通り各 EE のユーザ ID(IDx)，公開鍵(Pux)，MS 自身の秘密鍵(PrS)を所持する.

終端 EE から MS, MS から終端 EE では流れるパケットが異なるため，中間 EE では両方向のパケットを認証する必要がある．終端 EE から MS へのパケットの中継判定を行うために，認証情報(Eprs[Pux])をパケットに付加して送信する. このデータは MS の公開鍵で復号できるため，どの EE でも Pux を取得することが可能である．この Pux を用いることで，中間 EE においてもディジタル署名の検証を行うことが可能となる.

通常のディジタル署名の検証では,

・データが改ざんされていないこと

・データは，検証に使用した公開鍵と対になる秘密鍵によって署名されたこと

の 2 点を確認することが可能である. 認証情報 Eprs[Pux]から取り出されたものを公開鍵として利用することで，上記の 2 点に加えて,

該当するパケットは MS が認証した正規のユーザが生成したものであること

を確認することが可能となる．これにより，データの正当性が認められた場合は, 正規のユーザが作成したパケットであるとしてパケットを中継する.

MS から終端 EE へのパケットの中継判定は，初期情報として与えられた PuS を用いて MS からのパケットのディジタル署名を検証することによって行う．これにより，データの正当性が認められた場合は，MS が生成したパケットであると判断し，パケットを中継する.

表 1　各端末が所持している初期情報

Table.1 Initialization of each terminal.

EES	EE のユーザ ID(IDx)
EEN	EE の秘密鍵(Prx)
EEA	MS の公開鍵(PuS)
	※認証情報(Eprs[Pux])
MS	MS の秘密鍵(PrS)
	各 EE のユーザ ID(IDx)
	各 EE の公開鍵(Pux)　(x=1,2,3…)

※追加した初期情報

3.2 SKDP の提案

SKDP では，図 4 に示すように Key-REQ, Key-DIS, Key-IND の 3 つのパケットからなる. 以下に SKDP による鍵配送手順を示す.

(1) EE→MS：鍵配送要求(Key-Request)

終端 EE が MS に鍵配送の要求を行うためのパケットである．鍵配送要求に先立ち，鍵配送に用いる乱数 Rx を生成する. この Rx に加え，(3)で述べる鍵更新指示 Key-Indication によって鍵配送が行われる場合は, 取得の対象となるグループを記述した D を MS の公開鍵 Pux で暗号化した Epus[Rx|D]と，ユーザ ID である IDx を追加する．そして，ディジタル署名 Eprx[H(Epus[Rx|D]|IDx)]を付加し，認証情報 Eprs[Pux]を付加したものを鍵配送要求のパケットとして送信する.

Epus[Rx|D]|IDx|
Eprx[H(Epus[Rx|D]|IDx)]|Eprs[Pux]

このパケットを受信した中間 EE は，Eprs[Pux]を復号し，送信元端末の公開鍵 Pux

を得る．この Pux を用いてディジタル署名 Eprx[H(Epus[Rx]|IDx)]を検証する．これによりデータの正当性が認められた場合，パケットは MS が認証した秘密鍵をもつ端末が作成したものであるとし，中間 EE はパケットを中継する．データの正当性が認められなかった場合は，不正なパケットであるとしてパケットを破棄する．

MS がこのパケットを受信した時，中間 EE と同様にディジタル署名の検証を行う．その後 Epus[Rx|D]を復号し，IDx を元にユーザが所属しているグループを決定し，対応するグループ鍵を選択する．データの正当性が認められなかった場合，不正なパケットであるとしてパケットを破棄する．

(2) MS→EE：鍵配送(Key-Distribution)

MS での認証によって決定されたグループ鍵を配送するためのパケットである．終端 EE が所属するグループと，それに対応するグループ鍵を情報Ｄとし，(1)で取得した Rx とともに Rx で暗号化したデータ Erx[Rx|D]と，ディジタル署名 Eprs[H(Erx[Rx|D])]を終端 EE に送信する．

Erx[Rx|D]|
Eprs[H(Erx[Rx|D])]

このパケットを受信した中間 EE は，予め所持している MS の公開鍵 PuS を用いてディジタル署名を検証する．データの正当性が認められた場合，中間 EE はパケットを中継する．データの正当性が認められなかった場合，不正なパケットであるとしてパケットを破棄する．

終端 EE がこのパケットを受信した時，Erx[Rx|D]を復号し，自身が作成した Rx と比較して一致していた場合は，Ｄを取得する．データが認証できない，あるいは一定時間内に Key-DIS を受け取れなかった場合は，終端 EE はグループ鍵が取得できなかったものとして再度 Key-Request を送信する．

(3) MS→EE：鍵更新指示(Key-Indication)

グループ鍵が更新されたことを EE に通知し，グループ鍵の更新を指示するためのパケットである．鍵更新指示ではグループ鍵が更新されたグループに属する EE に対して送信される．このパケットは(2)の Key-Request と同様のパケットを作成し送信するが，このときのＤの内容は更新されたグループの情報のみとなる．中間 EE での認証も(2)と同様にして行う．

終端 EE がこのパケットを受信した時，Erx[Rx|D]を復号し，自身が作成した Rx と比較して一致していた場合は，Ｄを取得する．その後更新されたグループ鍵を取得するため，Ｄを用いて(1)の Key-Request を生成する．データの正当性が認められなかった場合，不正なパケットであるとしてパケットを破棄する．また，一定時間内に Key-Request が送信されなかった場合は，MS は正常に Key-Indication が送信できなかったものとして，パケットを再送する．

4. SKDP の評価

ここでは，3 章で提案した SKDP の有効性について述べる．

従来方式に置いては，中間 EE での認証が十分検討されていなかったため，鍵配送派パケットは中間 EE で認証を行わずに通過していた．SKDP では初期情報として認証情報を追加することにより，中間 EE でディジタル署名の検証を行うことが可能となる．また，パケットに認証情報を直接付加することにより，ユーザの

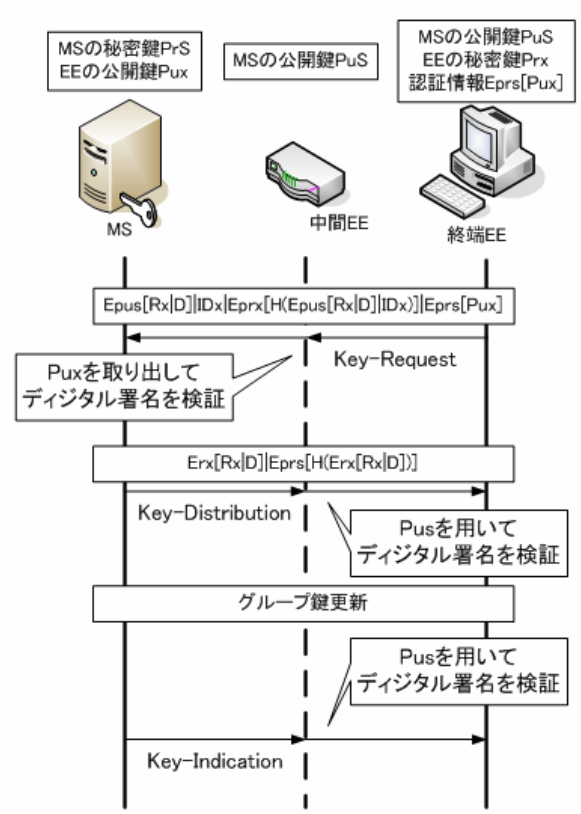

図 4　SKDP シーケンス

Fig.4 SKDP sequence.

追加や変更の影響を受けることなくパケット

の認証を行うことが可能となる．しかし，中間 EE においては End-to-End で行われる認証情報を参照することが出来ないため，対象となるパケットがシステムに属している正規の MS・EE のものであるかどうかを認証することとなる．ここでは，FPN における中間 EE での認証の有効性を述べる．

FPN で想定される鍵配送では，各 EE と MS との間での通信と限定されている．通信の片側が MS で固定されているため，送信元が MS であれば MS の公開鍵を，送信先が MS であればパケットに含まれている認証情報を参照して認証を行うことになる．このため，送信元/送信先の情報が上記以外の場合は不正パケットとして認証前に破棄することが可能である．このため，EE が他の端末に対して鍵配送パケットに偽装して情報を送信する場合，Key-Distribution または Key-Indication としてパケットを生成することになるが，中間 EE では MS の公開鍵を用いて認証が行われる．MS からのパケットのディジタル署名を生成できるのは秘密鍵を持つ MS のみであるため，認証により不正なパケットとして破棄される．上記の理由により，鍵配送パケットに偽装した不正なパケットが中間 EE を通過してネットワーク上に流れることを防止することが可能である．

次に認証情報の安全性について述べる．この情報は Key-Request に付加して送信されるため，MS の公開鍵を所持している EE であれば，中の Pux を取得することが可能である．しかし，この Pux ではディジタル署名の検証を行うことしか出来ないため，単に認証情報を付加しただけでは鍵配送パケットを偽造することは不可能である．よって，認証情報の追加によって鍵配送の安全性を損なうことはないと考えられる．

SKDP では全ての中間 EE においてディジタル署名の検証を行うため，中間 EE にかかる負荷が懸念される．EE は MS をルートとした木構造の形を取っているため，MS に近い EE ほどより大きな負荷が掛かると予想される．鍵配送は基本的に電源投入時であるため，実際の通信において大きな影響を与えるものではないと考えられる．また，全ての端末が同時に電源を投入することは考えにくいため，鍵配送自体も極端に集中して行われるものではないと考えられる．この点については，実装を行い十分な検討を行うことが必要である．

また，ユーザの追加や変更による影響を受けることなく中間 EE においてディジタル署名の検証を行う方法として，リポジトリを利用して必要に応じて公開鍵を取得する方法が考えられるが[8]-[11]，この方法では外部のリポジトリにアクセスしなければならず，この際に別の中間 EE が存在する可能性がある．これを通過するために新たな認証方法を規定するという課題が生じてしまう．リポジトリに自由にアクセスできる場合においても，通過する全ての中間 EE でリポジトリへのアクセスを行い公開鍵を取得するため，中間 EE となる EE が増えるとリポジトリへのアクセスが大幅に増加し，パフォーマンスに大きな影響を与えると考えられる．同様に公開鍵を用いてディジタル署名の検証を行うため，他へのアクセスがない分 SKDP の方がこのような用途には適していると考えられる．

5. むすび

本論文では，グループ鍵を配送する際に経路上に中間 EE が存在していても，認証によって中継の可否を決定できる鍵配送方式 SKDP を提案した．SKDP では従来の PKI 方式を利用し，認証情報の追加によって中間 EE での確実な認証を可能とした．

今後は提案方式の試作を行い，実用の上での有効性を検討していく予定である．同時に，中間 EE における認証による処理負荷の増加や，DoS 攻撃などによる極端な負荷への耐性などを検討していく予定である．

参考資料

[1] 渡邊，厚井，井手口，横山，妹尾 “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” 情報処理学会論文誌，Vol.38，No.4，1997

[2] 渡邊，井手口，笹瀬 “イントラネット閉域通信グループの物理的位置透過性を可能にする動的処理解決プロトコルの提案” 電子情報通信学会誌，Vol.J84-D-I，No.3，2001

[3] 荒井，鍛，伊藤，手塚，佐々木，“企業情報向けグループ暗号システム” 電子情報学会論文誌，Vol.40，No.12，1999

[4] S. Kent，R. Atkinson，“IP Authentication

Header” RFC2402，Dec. 1998

[5] S. Kent，R. Atkinson，“IP Encapsulating Security Payload (ESP)” RFC2406，Dec. 1998

[6] D. Harkins，D. Carrel，”The Internet Key Exchange (IKE)” RFC2409，Dec. 1998

[7] 渡邊，岡崎，朴，井手口，笹瀬 “イントラネット閉域通信グループの構築に適した安全な鍵配送方式とその運用管理方式” 電気学会論文誌 C, Vol.121-C, No.9, Sep 2001

[8] S. Boeyen，Entrust，T. Howes，Netscape，P. Richard，Xcert，” Internet X.509 Public Key Infrastructure Operational Protocols -LDAPv2” RFC2559，April. 1999

[9] S. Boeyen，Entrust，T. Howes，Netscape，P. Richard，Xcert，” Internet X.509 Public Key Infrastructure LDAPv2 Schema” RFC2587，June. 1999

[10] R. Housley，SPYRUS，P. Hoffman，IMC，”Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP” RFC2585，May. 1999

[11] D. Eastlake，IBM，O. Gudmundsson，TIS Labs，” Storing Certificates in the Domain Name System (DNS)” RFC2538，March. 1999