閉域通信グループにおける暗号通信方式の検討

増田 真也　　渡邊 晃

名城大学理工学部

1. はじめに

近年，ネットワークにおいて様々なセキュリティ上の脅威が問題となっており，それに伴いネットワークセキュリティが重要視されてきている．そのひとつとしてグループ外からの不正を防止するために，暗号技術を用いて閉域通信グループを構築する研究が行われている．

暗号技術を用いたセキュリティとして，IP層の技術であるIPsecが挙げられるが，セキュリティは強靭なものの，パケットの暗号化や完全性保証※1によってNA(P)Tやファイアウォールを通過できなくなることや，パケット長の増加によってフラグメントが発生することなどが問題とされている．また，[1]において既存システムに影響を与えないよう暗号化範囲を規定し，パケット長を変えずに暗号化を行う方式が提案されているが，TCP/UDPチェックサムの再計算を行うNA(P)Tを通過できないことや，本人性確認※2とパケットの完全性保証を考慮していないという課題がある．

そこで，本研究では[1]の提案をベースとし，既存システムに影響を与えずに，本人性確認とパケットの完全性保証も確実に行う暗号通信方式について提案する．本方式では，パケット長が変化しないため十分なスループットが期待できる上，NA(P)Tやファイアウォールを通過できる実用的なシステムを構築できる．

※1　パケットが改竄されていないことの保証
※2　正当な相手であることの保証

2. 既存技術とその課題

IPsec はIP層のセキュリティとして盛んに研究が行われているが，前述の通り多くの課題がある．暗号化を行う IPsec ESP トランスポートモード（以下IPsec ESP）の場合を考えると，図１のようにポート番号が暗号化されているのでファイアウォールを通過できない場合が多い．また，TCP/UDP チェックサムが暗号化範囲・完全性保証の範囲に含まれているためチェックサムの再計算を行う NA(P)T の通過はできない．この問題については，UDP ヘッダでカプセル化することで NA(P)T を通過させる NAT Traversal という対策が考案されており，有効な手段として普及しつつあるが，相互の IPsec 装置で対応している必要があり，カプセル部分は完全性保証に含まれない．その他，ヘッダの追加によるオーバヘッドやフラグメントの発生が課題として挙げられる．

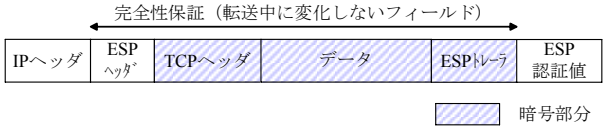


図１　IPsec ESP のパケットフォーマット（TCP の場合）

"A study on cipher communication system for closed communication group"
Shinya Masuda & Akira Watanabe
Faculty of Science and Technology, Meijo University

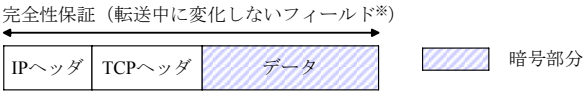
3. 提案方式

NA(P)T，ファイアウォールを通過でき，かつ本人性確認とパケットの完全性保証を，パケット長を変化させないまま実現する方式を提案する．本方式は，全て IP 層で行う．

提案方式では，図２のようにユーザデータ部分のみを暗号化の対象とする．すなわち，TCP/UDPヘッダを暗号化範囲から外すことで，NA(P)Tやファイアウォールを通過できるようにする．また，パケット長を変えずに暗号化するために，ブロック暗号のCFBモード※3を用いる．よって，提案方式によるフラグメントは発生しないため，高スループットが実現できる．

提案方式では，図２のように設定によってパケットの完全性保証に関わる処理を分ける．IP アドレスとポート番号を，NA(P)T なしの設定では完全性保証の範囲に含め，NA(P)T ありの設定では完全性保証の範囲に含めない．

※3　ブロック暗号をストリーム暗号として利用するモード



※　NA(P)Tありの設定
　　IPアドレス・ポート番号を含まない
　NA(P)Tなしの設定
　　IPアドレス・ポート番号を含む

図２　提案方式のパケットフォーマット（TCP の場合）

①　NA(P)T なしの設定

暗号化/復号の際は IV（Initialization Vector）をパラメータとして与える必要がある．IV は暗号化/復号で同じ値であり，使用する度に異なる値である必要がある．また，第三者には分からない値を用いることが望ましい．そこで，図３のように 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（IP アドレスとポート番号を含む．TCP/UDP チェックサムを除く．）の鍵付きハッシュ値を IV とすることで，暗号化/復号で同じ値であり，パケットごとに異なる値となる IV を生成することができる．IV 生成には鍵情報を含めているため，第三者に IV が知られることはない．

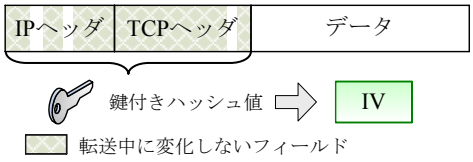


図３　IV(Initialization Vector)の生成

IPsec ESP ではヘッダを追加することで本人性確認とパケットの完全性保証を行っているが，提案方式ではパケット長を変えないためヘッダの追加はせず，TCP/UDP チェックサムを用いることで本人性確認とパケットの完全性保証を行う．本来 TCP/UDP チェックサムは，データの誤り検出を行うために用いるが，ここでは IP 層に独自の処理を追加することで本人性確認とパケットの完全性保証を行う．

送信側ではデータの暗号化を行う前に，TCP/UDP チェックサ

ムを検証して，上位層（TCP/UDP）から渡されたパケットが正しいことを確認したら，データの暗号化後，図４のように暗号データと IV を合わせたハッシュ値をデータの一部と見なして（疑似データと呼ぶ），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，同様の方法で作成した疑似データを含めて計算したチェックサムを検証し，復号後に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 IV 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．

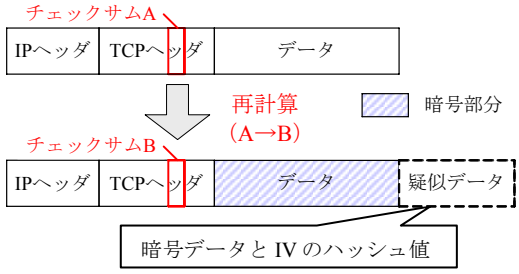


図４　チェックサムの再計算（TCP の場合）

パケットを改竄した場合，改竄者は TCP/UDP チェックサムを再計算するが，正当な者しか疑似データを作ることはできないので，改竄時に再計算を行うことはできない．この方式では，疑似データによって正当な相手であることが保証されるので本人性確認も実現する．

このように，疑似データを含めた TCP/UDP チェックサムの計算を行うことで，ヘッダの追加をせずに本人性確認と，暗号部分と IV 生成に用いるフィールドの完全性保証が実現する．

②　NA(P)T ありの設定

NA(P)T ありの設定では，IP アドレスとポート番号を IV 生成の範囲から外すことで NA(P)T の通過が可能となる．通信中に NA(P)T を通過する場合，IP アドレスやポート番号の変換によるチェックサムの再計算が行われるが，変換部分の差分計算を行う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[2]. この設定では IP アドレスとポート番号を IV 生成の範囲から外すため，別の方法で IP アドレスとポート番号の完全性保証を行う必要がある．例えば，図５のように暗号通信に先立って行う DPRP（Dynamic Process Resolution Protocol）[3]と本方式を組み合わせることで，IP アドレスとポート番号の完全性保証を実現できる．

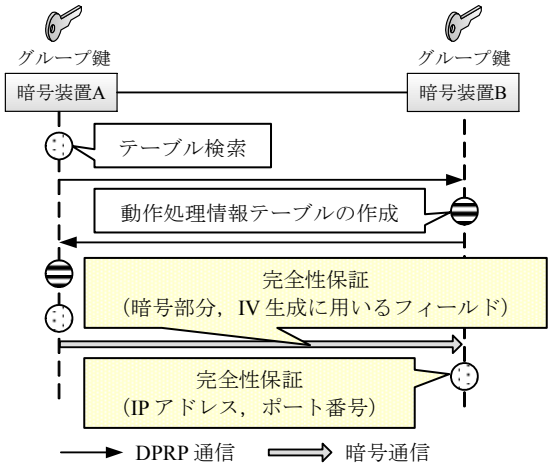


図５　DPRP と組み合わせたパケットの完全性保証

DPRP は，暗号通信に先立って暗号化/復号などの動作処理情報を記したテーブルを作成する．暗号通信は，そのテーブルを基に行う．動作処理情報テーブルには IP アドレスとポート番号の情報が含まれており，IP アドレスとポート番号のハッシュ値を検索キーとしてテーブル検索を行う．すなわち，受信側でテーブル検索にヒットしたら 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．

4.　実装

本研究では，提案方式をモジュール化して IP 層に実装する．パケットを IP 層で横取りして，モジュールに渡して処理をした後，差し戻すという流れで暗号通信を行う．開発・実装環境は IP 層の詳細な処理フローに関する情報が多い FreeBSD で行っている．現段階ではモジュールをカーネルに組み込む前に，ドライバを用いてテスト開発を行っている．暗号アルゴリズム，暗号エンジンは OpenSSL の AES_CFB モードを利用する．

5.　既存技術との比較検討

IPsec ESP と提案方式を６つの項目において比較した結果を表１に示す．

表１　IPsec ESP との比較

	機密性	本人性確認	完全性保証	NA(P)T	ファイアウォール	フラグメント
IPsec ESP	◎	◎	◎	△	△	×
提案方式	○	○	○	○	○	○

IPsec ESP は，TCP/UDP ヘッダを暗号化範囲に含めているが，特殊な処理・設定を行わないと NA(P)T やファイアウォールを通過できない．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．

提案方式は，TCP/UDP ヘッダを暗号化範囲に含めない代わりに，NA(P)T やファイアウォールを通過できる．また，パケット長が変化しないため，提案方式によるフラグメントは発生せず，高スループットを実現できる．

IPsec は，セキュリティは強靭だが NA(P)T やファイアウォールとの相性問題をはじめとした多くの課題がある．強力なセキュリティを要する場合は，これらの問題に注意しながら導入を検討することが重要である．提案方式は，既存システムに影響を与えないよう配慮しているため，実用性が高く比較的容易に導入できると考えられる．

6.　むすび

本稿では，既存システムに影響を与えずにオリジナルパケットとサイズを変えないで，本人性確認とパケットの完全性保証を行う暗号通信方式について提案した．

今後はモジュールをカーネルに組み込み，動作確認を行うと共に，既存技術との定量的な比較を行う予定である．

参　考　文　献

[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.04-025 Apr.1997

[2] K.Egevang, P.Francis “The IP Network Address Translator (NAT)” RFC 1631, May 1994.

[3] 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” 電子情報通信学会論文誌 VOL.J84-D-I No.3 Mar.2001