

IPSec 通信が可能なアドレス変換による IPv6 機器の位置透過なアクセス手法

黒木 秀和^{†1,†2} 井上 博之^{†3}
荻野 司^{†4} 石原 進^{†2}

近年, IP 通信機能が搭載された情報家電やセンサデバイスなどの機器が製品化されている。これらの機器は, 機器ユーザのネットワークに対応したアドレスが付与されるが, つねに同一の IP アドレスでこれらの機器と通信できれば, 遠隔から機器の保守, 操作, 監視を行うことが容易になる。筆者らは, 双方向のアドレス変換機構を持つアドレス変換装置を用い, 固定の IPv6 アドレスを用いた機器と他ノードの通信を可能とする手法 LTA6 を提案している。しかし, この手法では, 機器の保守, 操作, 監視を行う端末と機器の間で IPSec 通信ができないという問題があった。本稿では, これらの間の IPSec 通信を可能とするアドレス割当て手法を提案する。本手法では, アドレス変換の前後で ICMPv6, TCP, UDP ヘッダ内に含まれるチェックサムに変更が生じないように動的なアドレスを割当てることで, IPSec 通信を可能にしている。また, チェックサムの書き換えを不要とすることで, アドレス変換装置の処理負荷の低減を可能にしている。

IPSec Communications Capable Location Transparent Access Scheme with Address Translation for IPv6 Devices

HIDEKAZU KUROKI,^{†1,†2} HIROYUKI INOUE,^{†3} TSUKASA OGINO^{†4}
and SUSUMU ISHIHARA^{†2}

These days, information appliances, sensor devices, or etc. with IP communication functions are widely deployed. These devices are assigned an arbitrary address when there are connected with each device's user network. If a fixed IP address which is independent of locations of devices can be used to communicate with these devices at any time, remote accesses to the devices will be facilitated. We have proposed LTA6 which is a scheme for enabling a device with a fixed IPv6 address to communicate with any nodes by using an address translator which can be placed at arbitrary place on the Internet. However, there is a problem that the device nodes can not communicate with any nodes with IPSec in this scheme. In this paper, we propose a technique of address allocation for enabling IPSec communications between devices and any nodes. In this technique, IPSec communications are enabled by allocating an dynamic address which dose not change the checksum of included in ICMPv6, TCP, or UDP headers. Also, the load of address translator is reduced by eliminating to rewrite the checksum.

1. はじめに

近年, 家電, センサデバイス, 監視カメラなどの機器に IP 通信機能が搭載され, 機器を製造したベンダ

(機器ベンダ) による遠隔からの機器の保守, 操作, 監視などに利用されるようになってきている。遠隔からの機器へのアクセスを実現するには, 機器の現在の IP アドレスをつねに把握する必要がある。しかし, 機器が設置されるネットワークやその上位ネットワークは, 機器ユーザごとに異なり, 機器ユーザの引越しや利用する ISP (Internet Service Provider) の変更によって変化する。これに伴って, 機器のアドレスも変化する。このため, 機器ベンダは, 変化する機器のアドレスを機器の出荷前に知ることは困難である。

機器の設置場所とは独立した固定の接続情報で機器と通信可能であれば, 機器ベンダは, 機器のアドレス

†1 株式会社ユビテック ユビキタス研究所
Ubiquitous Laboratories, Ubiteq, INC.

†2 静岡大学創造科学技術大学院
Graduate School of Science and Technology, Shizuoka University

†3 広島市立大学情報科学研究科
Graduate School of Information Sciences, Hiroshima City University

†4 株式会社ユビテック
Ubiteq, INC.

が変化する度にその接続情報を変更する必要がなくなり、機器の保守、操作、監視などを低コストで実現できる。ただし、機器ベンダが機器に割当てた固定の接続情報を用いて機器に対する不正アクセスが行われた場合、機器ベンダの責任が問われる可能性がある。このため、機器ベンダは接続情報を用いた通信をつねに監視・制御できる必要がある。

筆者らは、つねに固定の IPv6 アドレスで機器にアクセス可能な技術として、Location Transparent Access to a lightweight IP device through an IPv6 fixed address (LTA6)¹⁾を提案している。LTA6 では、機器ベンダのネットワークに設置したアドレス変換装置で、固定アドレスと機器の設置場所におけるアドレスの相互変換を行うことで、固定の IPv6 アドレスによる機器へのアクセスを実現している。機器には通常の IPv6 機能に加えてアドレス変換装置にアドレスを登録する機能のみを持たせればよい。また、固定の IPv6 アドレスを用いた通信は、つねにアドレス変換装置を経由するため、不正アクセスの監視・制御を容易に行うことができる。

しかし、LTA6 では、機器の保守、操作、監視を行う端末と機器の通信の経路途中のアドレス変換装置上で IPv6 アドレスの変換を行うため、端末と機器の末端どうしの間で IP Security (IPSec)²⁾通信を行うことができないという問題があった。これは、IPSec による暗号化や認証の対象である ICMPv6、TCP、UDP ヘッダ内に含まれるチェックサムの計算に、送り元と宛先の IPv6 アドレスを使用するインターネットチェックサム^{3),4)}を用いることが原因である。このため、アドレスを変換する際にチェックサムも計算し直す必要があるが、IPSec を用いたパケットではチェックサムの部分が暗号化または認証の対象となっているため、変更は不可能である。それゆえ、LTA6 では、端末-機器間で直接的な IPSec 通信を行うことができず、端末-アドレス変換装置間、機器-アドレス変換装置間でそれぞれ異なる IPSec 通信を行う必要があった。

本稿では、インターネットチェックサムで計算されるチェックサムが、端末-アドレス変換装置間、機器-アドレス変換装置間のそれぞれでつねに同一となるように、LTA6 で利用するアドレスを選択する方法を提案する。これにより、アドレス変換装置におけるアドレス変換の際に、ICMPv6、TCP、UDP ヘッダ内のチェックサムを変更する必要がなくなる。このため、端末と機器の末端どうしの間で IPSec 通信を行うことが可能となる。また、各パケットごとに、ICMPv6、TCP、UDP ヘッダを内包するか否かを判別したり、チェックサ

ムを変更したりする処理が不要になるため、アドレス変換装置上におけるパケットの変換処理はアドレス変換のみとなり、処理負荷を低減できる。パケットに含まれる ICMPv6、TCP、UDP ヘッダを識別し、チェックサムを変更する処理は比較的重いいため、この低減効果は大きい。

以下、2 章では関連技術について述べ、3 章では LTA6 について述べる。4 章では IPSec 通信を可能とする LTA6 における拡張したアドレス割当て手法について述べ、5 章ではその検討を行う。最後に、6 章でまとめを行う。

2. 関連技術

通信の途中でアドレス変換が行われる場合において IPSec 通信を実現する技術として、IPSec の Network Address Translation (NAT)^{5),6)} 越えを実現する IPSec Network Address Translation Traversal (IPSec NAT-Traversal)⁷⁾⁻⁹⁾がある。また、IPSec のトンネルモードを応用することにより通信途中でアドレス変換が行われても IPSec 通信が可能となる場合がある。これらについて述べる。

2.1 IPSec NAT-Traversal

IPSec NAT-Traversal は、NAT を利用している環境で IPSec 通信を可能とする技術である。IPSec NAT-Traversal を用いると、NAT 環境に存在するノードは、TCP や UDP などの上位レイヤのデータに対して IP Encapsulating Security Payload (ESP)¹⁰⁾で暗号化を行って ESP ヘッダや認証データを付加したパケットを生成し、これを UDP のデータとして終点ポート番号が 500 または 4500 番の UDP ヘッダでカプセリングして送信する。UDP でカプセリングされたパケットを受信した IPSec 通信の対向ノードは、UDP ヘッダでカプセリングされた ESP ヘッダ以降のデータを復号化して上位レイヤのデータを取り出す。このように動作することで、NAT によるアドレス変換やポート番号の変換が行われても、ESP で暗号化された上位レイヤの TCP や UDP などのヘッダに含まれるチェックサムの変更を不要とし、IPSec 通信を可能にしている。なお、IPSec NAT-Traversal では、ESP のみの IPSec 通信が可能で、IP Authentication Header (AH)¹¹⁾を用いた IPSec 通信は不可能である。

しかし、IPSec NAT-Traversal は、IPSec 通信を行う端末のノードに UDP カプセリング処理が必要となり、終点ポート番号が 500 または 4500 番の UDP パケットに対する特別な処理が必要である。さらに、UDP でカプセリングすることでパケット長が増加し、

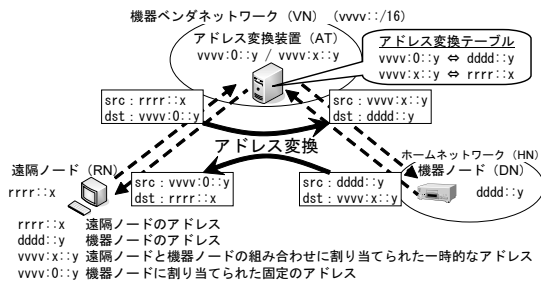


図 1 LTA6 の概要

Fig.1 Overview of LTA6.

通信の効率が低下する。

2.2 IPSec トンネルモードの応用

セキュリティゲートウェイを介さない末端のノードどうしのIPSec通信において、トランスポートモードではなくトンネルモードを用いることで、通信の途中でアドレス変換が行われてもIPSec通信が可能となる。この方法を用いると、あるノードが通信相手に対して送信する通常のIPパケット全体をESPで暗号化を行ってESPヘッダや認証データを付加したパケットを生成し、これの先頭にIPヘッダを付加することでトンネリングを行って送信する。そして、受信側では通常のトンネルモードのIPSec通信として処理を行う。このように動作することで、アドレス変換の前後でトンネリングの内部のIPパケットに対する変更を不要とし、IPSec通信を可能にしている。なお、この方法も、ESPのみのIPSec通信が可能で、AHを用いたIPSec通信は不可能である。

しかし、このIPSecトンネルモードを応用した方法は、IPSec通信を行う末端のノードにトンネリング処理が必要となり、ノードに2つのアドレスを用意する必要がある。さらに、トンネリングすることでパケット長が増加し、通信の効率が低下する。

3. LTA6

LTA6は、図1のように、機器ベンダネットワークのネットワークプレフィックスに含まれるアドレスを固定アドレスとして機器ベンダネットワーク上のアドレス変換装置に設定し、このアドレス変換装置上で受信する通信パケットの宛先アドレス（以下、宛先）および送り元アドレス（以下、送り元）を変換することにより、固定アドレスで機器にアクセスすることを可能とする。LTA6は以下の2つの特徴を持つ。

- i) 機器に必要な追加機能が少なく、処理負荷も少ない。
- ii) 通信は機器ベンダが管理するノードを経由する

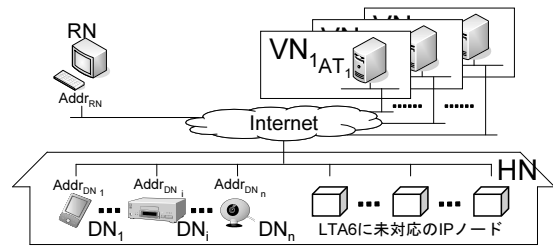


図 2 LTA6 のシステム構成

Fig.2 System overview of LTA6.

ため、不正な通信の遮断が可能。

3.1 LTA6 のシステム構成

LTA6のシステムは、図2に示すように、機器ノード (Device Node: DN)、遠隔ノード (Remote Node: RN)、アドレス変換装置 (Address Translator: AT) の各ノードで構成される。

DNは、機器ベンダから出荷される機器であり、機器ユーザのホームネットワーク (Home Network: HN) に接続されている。HNはインターネットに接続され、LTA6に対応した1つ以上のDNおよびそれ以外のIPノードが接続される。RNは、DNと通信を行うインターネット上の遠隔に設置された任意のIPノードである。DNとRNには、それぞれインターネット上の任意のノードと通信可能なIPv6アドレス $Addr_{DN}$ および $Addr_{RN}$ が設定されている。ATは、アドレスを変換と通信監視を行うための装置であり、機器ベンダに割り当てられたIPv6ネットワークプレフィックスを持つ機器ベンダネットワーク (Vendor Network: VN) に接続される。VNおよびATは、機器ベンダごとに独立して存在する。

3.2 固定アドレスおよび一時アドレス

LTA6では、 $Addr_{DN}$ と $Addr_{RN}$ 以外に、以下の2種類のIPv6アドレスを使用する。

- DNに固定で割り当てるIPv6アドレス (固定アドレス) $FixAddr_{DN}$
- RN-DN間の組み合わせに一時的に割り当てるIPv6アドレス (一時アドレス) $TmpAddr_{RN, DN}$

これらは、機器ベンダが割り当てを受けたIPv6ネットワークのプレフィックスを持ち、すべてATのアドレスとして設定される。すなわち、これらのアドレスを宛先とするパケットは、AT (VN) にルーティングされる。

機器ベンダに割り当てられたIPv6ネットワークのプレフィックス長を32ビットとした場合の固定アドレス及び一時アドレスの構成を図3に示す。それぞれの下位64ビットは、DNの機器IDである。DNの機器

機器ノード(DN)用の固定アドレス(FixAddr _{DN})		
機器ベンダに割り当てられた IPv6プレフィックス	000 000 固定	DNの機器ID (DNのMACアドレスから生成)
遠隔ノード(RN) - 機器ノード(DN)の組み合わせに対する一時アドレス(TmpAddr _{RN, DN})		
機器ベンダに割り当てられた IPv6プレフィックス	000 000 以外	DNの機器ID (DNのMACアドレスから生成)
32ビット	32ビット	64ビット

図 3 固定アドレスおよび一時アドレスの例
Fig. 3 Example of a fixed address and a temporary address.

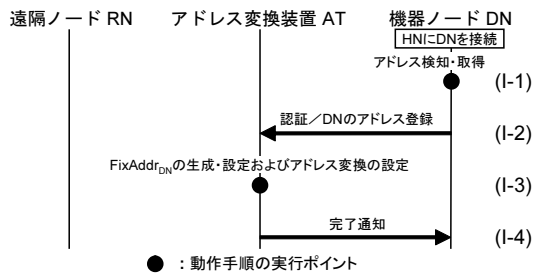


図 4 DN を HN へ接続する時の初期動作
Fig. 4 Initial procedure of connecting DN to HN.

ID は、IPv6 アドレス仕様¹²⁾ のインタフェース ID であり、DN のネットワークインタフェースの MAC アドレスから生成される。中間の 32 ビットは、固定アドレスの場合はすべてのビットで 0 であり、一時アドレスの場合は 0 でないビットを少なくとも 1 つ含んでいる。一時アドレスは、異なる RN-DN の組み合わせごとに TmpAddr_{RN, DN} が異なるように中間の 32 ビットがラウンドロビンで割り当てられる。

3.3 LTA6 の動作手順

LTA6 の動作手順を以下の 3 つに分けて述べる。

- DN を設置する時の初期動作
- RN から通信を開始する時の動作
- DN から通信を開始する時の動作

なお、以下に述べる動作手順において、アドレス変換の前後でパケットのサイズに増減はない。

3.3.1 DN を設置する時の初期動作 (図 4)

DN には、AT の FQDN などの AT へアクセスするための情報 (以下、AT アクセス情報) が出荷時に機器ベンダによって設定されている。HN に DN が接続され、ルータ広告¹³⁾ や DHCPv6¹⁴⁾ などにより、DN に新しい IPv6 アドレスが設定されると、以下の処理が行われる。

- (I-1) DN は、Addr_{DN} とネットワークインタフェースの MAC アドレスを取得する。
- (I-2) DN は、AT アクセス情報を用いて AT に接続し、AT-DN 間で適切な認証を行った後に Addr_{DN} および MAC アドレスを AT に送信して DN のアドレス登録を行う。この通信の方法について

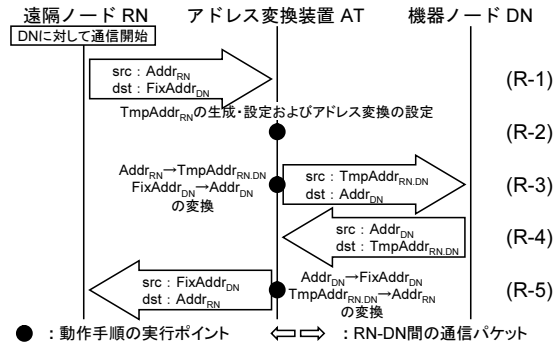


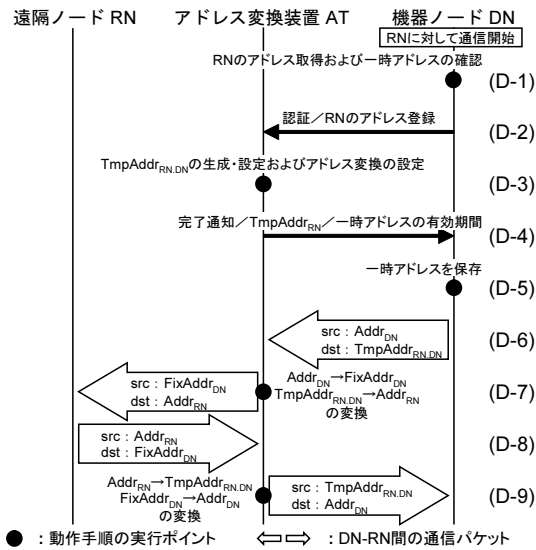
図 5 RN から通信を開始する場合の動作
Fig. 5 Procedure of communication from RN to DN.

はここでは問わない。

- (I-3) AT は、DN の MAC アドレスから DN に割当てて固定アドレス FixAddr_{DN} を決定して自身に設定し、Addr_{DN} ↔ FixAddr_{DN} のアドレス変換を設定する。
- (I-4) AT は、DN のアドレス登録に対する完了通知を DN に送信する。

3.3.2 RN から通信を開始する時の動作 (図 5)

- (R-1) RN は、FixAddr_{DN} を宛先とするパケットを送信する。このパケットは VN にルーティングされ、AT に FixAddr_{DN} が設定済みの場合は AT が受信し、未設定の場合は RN に到達不能エラーが返される。
- (R-2) AT は、送り元が Addr_{RN}、宛先が FixAddr_{DN} のパケットを受信すると、Addr_{RN} と FixAddr_{DN} に対応する一時アドレス TmpAddr_{RN, DN} が自身に設定済みか確認する。未設定の場合、AT は、一時アドレス TmpAddr_{RN, DN} を決定して自身に設定し、TmpAddr_{RN, DN} ↔ Addr_{RN} のアドレス変換を設定する。
- (R-3) AT は、受信パケットの送り元が Addr_{RN} 宛先が FixAddr_{DN} である場合、送り元を TmpAddr_{RN, DN} 宛先を Addr_{DN} に変換し、DN に送信する。また、このとき ICMPv6、TCP、UDP ヘッダ内のチェックサムを更新する。
- (R-4) DN は、受信したパケットに対する応答として、その送り元である TmpAddr_{RN, DN} を宛先とするパケットを送信する。このパケットは VN にルーティングされ、AT が受信する。
- (R-5) AT は、受信パケットの送り元が Addr_{DN} 宛先が TmpAddr_{RN, DN} である場合、送り元を FixAddr_{DN} 宛先を Addr_{RN} に変換し、RN に送信する。また、このとき ICMPv6、TCP、UDP ヘッダ内のチェックサムを更新する。



● : 動作手順の実行ポイント
 ⇔ : DN-RN間の通信パケット
 図 6 DN から通信を開始する場合の動作
 Fig. 6 Procedure of communication from DN to RN.

3.3.3 DN から通信を開始する時の動作 (図 6)

- (D-1) DN は、DNS などによって $Addr_{RN}$ を取得する。DN は、 $Addr_{RN}$ をキーとして有効期限内の $TmpAddr_{RN, DN}$ が存在するか確認する。存在する場合は、(D-6) 以降の処理を行う。
- (D-2) DN は、AT アクセス情報を用いて AT に接続し、AT-DN 間で適切な認証を行った後に $Addr_{RN}$ および $Addr_{DN}$ を AT に送信して RN のアドレス登録を行う。この通信の方法についてはここでは問わない。
- (D-3) AT は、 $Addr_{DN}$ をキーとして (I-3) で設定した $FixAddr_{DN}$ を割り出し、 $Addr_{RN}$ と $FixAddr_{DN}$ に対応する一時アドレス $TmpAddr_{RN, DN}$ が自身に設定済みか確認する。未設定の場合、AT は、一時アドレス $TmpAddr_{RN, DN}$ を決定して自身に設定し、 $TmpAddr_{RN, DN} \leftrightarrow Addr_{RN}$ のアドレス変換を設定する。
- (D-4) AT は、RN のアドレス登録に対する完了通知と $TmpAddr_{RN, DN}$ および一時アドレスの有効期間を DN に送信する。
- (D-5) DN は、 $TmpAddr_{RN, DN}$ を $Addr_{RN}$ と対応づけて、現在日時に一時アドレスの有効期間を加算した有効期限とともに自身に記録する。
- (D-6) DN は、 $TmpAddr_{RN, DN}$ を宛先とするパケットを送信する。このパケットは VN にルーティングされ、AT が受信する。
- (D-7) (R-5) に同じ。
- (D-8) RN は、受信したパケットに対する応答として、

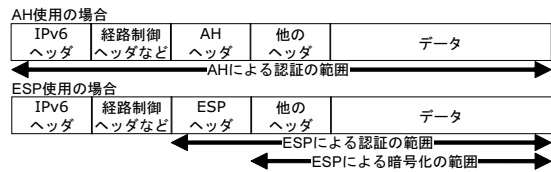


図 7 IPsec による IPv6 パケットの認証と暗号化の範囲
 Fig. 7 Authenticated field and encrypted field in IPv6 packets by IPsec.

その送り元である $FixAddr_{DN}$ を宛先とするパケットを送信する。このパケットは VN にルーティングされ、AT が受信する。

(D-9) (R-3) に同じ。

3.4 IPsec 利用にともなう問題点

LTA6 では、AT においてアドレス変換を行うパケットに ICMPv6、TCP、UDP のいずれかのヘッダが含まれる場合、これらのヘッダ内のチェックサムを再計算して変更する必要がある。なぜなら、これらのチェックサムは、送り元と宛先のアドレスを用いて算出されており、アドレス変換により変化するためである。アドレス変更に合わせてチェックサムを変更しない場合、宛先の RN や DN でパケットが破棄されてしまう。

しかし、IPsec によって暗号化または認証情報が付加されているパケットは、通信途中でその中に含まれる ICMPv6、UDP、TCP ヘッダ内のチェックサムを変更できない。このため、LTA6 を用いた場合、RN-DN 間の直接的な IPsec 通信が不可能という問題がある。

RN-AT 間と AT-DN 間で別々の IPsec 通信を行うことで AT 内を除き IPsec 通信が可能となるが、暗号化と復号化を AT で同時に行うために、AT における IPsec の処理負荷が大幅に増加する。また、AT が不正アクセスを受けて乗っ取られた場合、2 つの IPsec 通信の間の暗号化されていないパケットが盗聴される危険がある。

4. IPsec 通信可能なアドレス割当て手法

4.1 IPsec とアドレス変換

IPv6 パケットに IPsec を適用した場合、AH や ESP によって認証や暗号化がなされる範囲を図 7 に示す。AH を用いるとパケットのすべてが認証される範囲となるため、アドレス変換を行うとパケットが改竄されたと判断され通信ができない。一方、ESP のみを用いた場合は ESP ヘッダ以降が認証と暗号化の範囲となるため、ESP ヘッダ以降のヘッダやデータにアドレスに依存する部分がない場合は、アドレス変換が可能となる。また、アドレスに依存する部分が ESP ヘッダ以降に存在する場合でも、アドレス変換によって ESP

表 1 IPsec 通信の packets に対するアドレス変換の可否
Table 1 Possibility of address translation of packets in IPsec communications.

	AH	トランスポートモード	トンネルモード
		ESP	ESP
ICMPv6	×	△	○
TCP	×	△	○
UDP	×	△	○

○ : アドレス変換可能
△ : チェックサムが変化しなければアドレス変換可能
× : アドレス変換不可

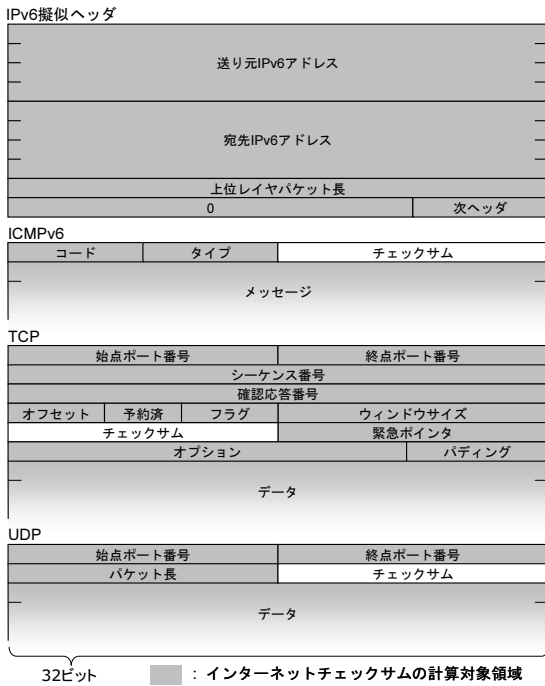


図 8 IPv6 擬似ヘッダおよびインターネットチェックサムの計算対象領域
Fig. 8 Pseudo-header for IPv6 and target areas of internet checksum calculation.

ヘッダ以降に変更が生じない場合は、アドレス変換が可能となる。

ICMPv6, TCP, UDP は、これらのヘッダにアドレスを用いて計算されるチェックサムを含んでいる。AH または ESP を用いた IPsec 通信の packets に対するアドレス変換の可否を表 1 に示す。なお、トンネルモード ESP は、2.2 節のトンネルモードを応用した場合の IPsec 通信である。

4.2 インターネットチェックサム

IPv6 の場合、ICMPv6, TCP, UDP ヘッダ内のチェックサムを求めするために用いられるインターネットチェックサムは、図 8 に示す IPv6 擬似ヘッダ¹⁵⁾ と ICMPv6, TCP, UDP パケット内の計算対象領域を

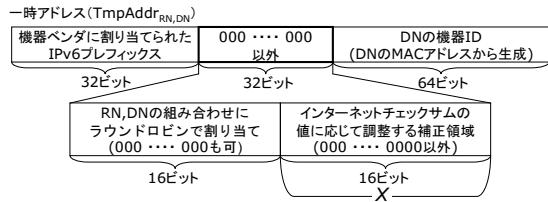


図 9 インターネットチェックサム補正領域を持つ一時アドレス
Fig. 9 A temporary address with a correction area for internet checksum.

用いて計算を行う。インターネットチェックサムの計算手順を以下に示す。

- 計算対象領域を、先頭から 16 ビットごとに分割する。
- 分割した各 16 ビット列の 1 の補数和を得る。
- 1 の補数和の 1 の補数を得る。

このようにして算出される値が、ICMPv6, TCP, UDP ヘッダ内のチェックサムとして用いられる。ただし、算出される値が 0x0000 の場合、0x0000 の代わりに 0xFFFF がチェックサムとして用いられる。一方、iii) までの計算で算出される値が 0xFFFF となるのは、分割された各 16 ビット列がすべて 0x0000 の場合である。しかし、計算対象領域のすべてのビットが 0 であるパケットは現実的に存在しないので、算出される値が 0xFFFF になることはない。このため、iii) までの計算で算出される値が 0x0000 の場合、0x0000 に代わりに 0xFFFF をチェックサムとして用いても、混同することはない。

4.3 一時アドレスの割当て手法

4.2 節から解るように、分割された各 16 ビット列のいずれかを自由に変更可能となれば、インターネットチェックサムで算出される値を任意に決定することができる。この場合、ESP のみによる IPsec 通信を行うことが可能となる。

LTA6 では、DN のアドレス Addr_{DN}, RN のアドレス Addr_{RN} および固定アドレス FixAddr_{DN} は、固定であるか RN や DN の設置場所によって変化するため、自由に決定できない。しかし、一時アドレス TmpAddr_{RN, DN} は、AT で自由に決定できる。

図 9 に示すように、TmpAddr_{RN, DN} の 33~64 ビット目の 32 ビットのうち、49~64 ビット目の 16 ビットをインターネットチェックサム補正領域とすると、インターネットチェックサム補正領域を調整することで、一時アドレス TmpAddr_{RN, DN} を送り元または宛先に持つパケット内の ICMPv6, TCP, UDP ヘッダ内のチェックサムを任意の値にできる。また、33~48 ビット目の 16 ビットは、異なる RN, DN の組み合わせ

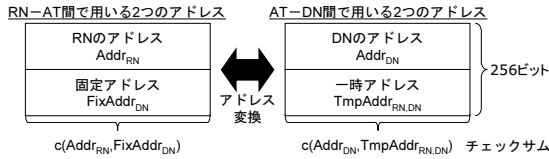


図 10 アドレス変換で変化する部分のインターネットチェックサム
Fig. 10 Internet checksum of an area which is changed before and behind address translation.

せに対してラウンドロビンで割当てすることで、同時に複数の一時アドレスを AT に設定できるようにする。49～64 ビット目の 16 ビットすべてが 0 になることはないとする、LTA6 において 33～64 ビット目の 32 ビットすべてが 0 にならないことに合致する。以降、49～64 ビット目の 16 ビットで構成される 16 ビットのビット列を X とする。

インターネットチェックサムの算出では交換則および結合則が成立する。また、LTA6 でアドレス変換の前後においてチェックサム以外で変化するのを送り元および宛先のアドレスだけである。このため、関数 $c(Addr_1, Addr_2)$ を $Addr_1, Addr_2$ の 2 つのアドレスを合わせた 256 ビットを計算対象領域として、4.2 節のインターネットチェックサムの計算手順 i)～iii) で算出される値と定義すると、図 10 に示す $c(Addr_{DN}, TmpAddr_{RN,DN})$ と $c(Addr_{RN}, FixAddr_{DN})$ が等しくなるように $TmpAddr_{RN,DN}$ を決定すれば、アドレス変換の前後において ICMPv6, TCP, UDP ヘッダ内のチェックサムに変更は生じないことになる。

$TmpAddr_{RN,DN}$ のインターネットチェックサム補正領域をすべて 0 としたものを $TmpAddr'_{RN,DN}$ とすると、アドレス変換の前後で ICMPv6, TCP, UDP ヘッダ内のチェックサムが変化しないビット列 X は、以下のようになる。なお、簡単のため、 $Addr_{DN}, Addr_{RN}, FixAddr_{DN}, TmpAddr_{RN,DN}, TmpAddr'_{RN,DN}$ を、それぞれ D, R, F, T, T' とする。また、 \oplus は 1 の補数における加算記号、ビット列 n に対して \bar{n} は n をビット反転させたものとする。

$$X = \overline{c(R, F)} \oplus c(D, T') \quad (1)$$

これを、16 ビット無符号の加減算式で表すと以下のようになる。

A) $\overline{c(R, F)} > \overline{c(D, T')}$ の場合

$$X = \overline{c(R, F)} - \overline{c(D, T')} \quad (2)$$

B) $\overline{c(R, F)} \leq \overline{c(D, T')}$ の場合

$$X = \overline{c(R, F)} + (0xFFFF - \overline{c(D, T')}) \quad (3)$$

X を上記のようにすることで、アドレス変換の前後で ICMPv6, TCP, UDP ヘッダ内のチェックサムが変化しないことの証明を以下に示す。

X は、関数 $c()$ のインターネットチェックサムにおいて 16 ビット単位に分割したうちの 1 つであり、 X および T' の定義から

$$c(D, T) = \overline{\overline{c(D, T')}} \oplus X \quad (4)$$

$$= \overline{c(D, T')} \oplus \bar{X} \quad (5)$$

$$= c(D, T') \oplus \bar{X} \quad (6)$$

である。 X に式 (1) を代入すると、

$$c(D, T) = c(D, T') \oplus \overline{\overline{c(R, F)} \oplus c(D, T')} \quad (7)$$

$$= c(D, T') \oplus (\overline{c(R, F)} \oplus \overline{c(D, T')}) \quad (8)$$

$$= c(D, T') \oplus (c(R, F) \oplus \overline{c(D, T')}) \quad (9)$$

$$= c(R, F) \oplus (c(D, T') \oplus \overline{c(D, T')}) \quad (10)$$

$$= c(R, F) \quad (11)$$

となる。したがって、 X を式 (1) のようにした $TmpAddr_{RN,DN}$ を用いると、アドレス変換の前後で ICMPv6, TCP, UDP ヘッダ内のチェックサムが変化しないことが分かる。

図 9 で示したように、LTA6 における一時アドレスは 33～64 ビットのいずれかが 1 である必要がある。なぜなら、この部分のビットを全て 0 にしたものは一時アドレスではなく、DN 用の固定アドレスとなるからである。 X は一時アドレス T の 49～64 ビット目を占めるので、 X が 0x0000 でなければ、一時アドレス T は先の条件を満たす。そこで、以下で式 (1) で得られる X が 0x0000 にならないことを示す。

R および F は通信可能なアドレスであるため、すべてのビットが 0 になることはない。したがって、 R, F の 16 ビットごとの 1 の補数和 $\overline{c(R, F)}$ が、0x0000 となることはない。0x0000 以外の値と任意の値の 1 の補数和が 0x0000 となることはないので、式 (1) より、 X が 0x0000 になることはない。

LTA6 に本手法を併用して一時アドレスを割当てすることで、アドレス変換の前後で ICMPv6, TCP, UDP ヘッダ内のチェックサムが変化しない。このため、RN-DN 間の直接的な ESP のみの IPsec 通信が可能となり、RN-AT 間、AT-DN 間で個別の IPsec 通信を行う必要がなくなるとともに、AT において RN-DN 間の通信内容が漏洩することもない。また、各パケット内に含まれる ICMPv6, TCP, UDP を判別する処理や、アドレス変換と同時にチェックサムを再計算して変更する処理が不要になる。このため、アドレス変換装置の処理負荷が低減される。

5. 検 討

5.1 AH ヘッダ

本手法による AH を用いた IPSec 通信は不可能であり、本手法は ESP のみの IPSec 通信に適用することができる。しかし、ESP が AH と同等の機能を持つため、AH は、IPSec における必須の機能ではなくなっている。IP ヘッダのアドレスを除いた部分や経路制御ヘッダなどの改竄をチェックする場合を除き、今後 AH が用いられることは少なくなると考えられる。このため、IP より上位レイヤの通信内容を暗号化し認証データを付加して通信する用途において、AH が使用できないことは重要な問題とならない。

5.2 鍵交換プロトコルとの連携

DN では、RN に対して通信を開始する場合、 Addr_{RN} ではなく、 $\text{TmpAddr}_{\text{RN, DN}}$ と通信をしている。このため、DN が RN に対して IPSec 通信を開始する場合、 Addr_{RN} 宛の通信に対して IPSec を適用するセキュリティポリシーの代わりに、 $\text{TmpAddr}_{\text{RN, DN}}$ 宛の通信に対して IPSec を適用するセキュリティポリシーを設定する必要がある。また、RN から IPSec 通信を開始する場合、DN は、 $\text{TmpAddr}_{\text{RN, DN}}$ を予期できない。このため、DN は外部からの IPSec 通信の要求についてはすべて受諾するように動作する必要がある。

5.3 関連技術との比較

IPSec NAT-Traversal および IPSec トンネルモードの応用ともに、機器にトンネリングやカプセリングの処理が必要である。このため、機器の処理負荷が増大し、通信の効率が悪くなる。しかし、本稿で提案するアドレス割当て手法を併用した LTA6 では、機器にトンネリングやカプセリングの処理は不要である。また、IPSec による通信量の増加は、ESP ヘッダと関連する認証データのみであり、関連技術に比べて通信の効率がよい。

6. ま と め

本稿では、筆者らが提案する機器ベンダネットワークに設置したアドレス変換装置を用いることで機器に対して固定のアドレスでアクセス可能とする LTA6 において、機器と機器の保守、操作、監視を行う遠隔の端末間の IPSec 通信を可能とするアドレス割当て手法を提案した。本手法では、アドレス変換の前後で ICMPv6、TCP、UDP ヘッダ内のチェックサムが変化しないアドレスを動的に割当てることにより、LTA6 でアドレス変換を行う際にチェックサムの変更を不要にしている。またチェックサムの変更が不要になるこ

とで、各パケットごとに、ICMPv6、TCP、UDP ヘッダを内包するか否かを判別する処理や、チェックサムを計算する処理が不要となり、アドレス変換装置の処理負荷が低減される。

今後の課題として、TCP、UDP 以外のトランスポート層プロトコルへの適用や、本手法を追加した LTA6 の実装とその検証があげられる。

参 考 文 献

- 1) 黒木秀和, 井上博之, 荻野 司, 石原 進: LTA6: 双方向アドレス変換装置による IPv6 固定アドレスを介した軽量 IP 機器への位置透過なアクセス手法, 信学技報, Vol.107, No.314, pp. 49-54 (2007).
- 2) Kent, S. and Seo, K.: Security Architecture for the Internet Protocol, RFC 4301 (2005).
- 3) Braden, R.T., Borman, D.A. and Partridge, C.: Computing the Internet checksum, RFC 1071 (1988).
- 4) Braden, R.T., Borman, D.A. and Partridge, C.: Incremental updating of the Internet checksum, RFC 1141 (1990).
- 5) Srisuresh, P. and Holdrege, M.: IP Network Address Translator (NAT) Terminology and Considerations, RFC 2663 (1999).
- 6) Srisuresh, P. and Egevang, K.: Traditional IP Network Address Translator (Traditional NAT), RFC 3022 (2001).
- 7) Aboba, B. and Dixon, W.: IPsec-Network Address Translation (NAT) Compatibility Requirements, RFC 3715 (2004).
- 8) Kivinen, T., Swander, B., Huttunen, A. and Volpe, V.: Negotiation of NAT-Traversal in the IKE, RFC 3947 (2005).
- 9) Huttunen, A., Swander, B., Volpe, V., DiBurro, L. and Stenberg, M.: UDP Encapsulation of IPsec ESP Packets, RFC 3948 (2005).
- 10) Kent, S.: IP Encapsulating Security Payload (ESP), RFC 4303 (2005).
- 11) Kent, S.: IP Authentication Header, RFC 4302 (2005).
- 12) Hinden, R. and Deering, S.: IP Version 6 Addressing Architecture, RFC 4291 (2006).
- 13) Thomson, S. and Narten, T.: IPv6 Stateless Address Autoconfiguration, RFC 2462 (1998).
- 14) Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C. and Carney, M.: Dynamic Host Configuration Protocol for IPv6 (DHCPv6), RFC 3315 (2003).
- 15) Deering, S. and Hinden, R.: Internet Protocol, Version 6 (IPv6) Specification, RFC 2460 (1998).