次世代インターネットに向けた動的な匿名閉域通信方式の提案

小川 猛志† 小林 裕太† 宮保 憲治†

†東京電機大学情報環境学部〒270-1355 千葉県印西市武西学園台 2-1200

E-mail: t.ogawa@mail.dendai.ac.jp

あらまし 現状のインターネットには，DoS 攻撃や IP アドレスのなりすまし・名寄せなどの問題がある．本稿では，次世代のインターネットの構築に向け，上記問題を根本的に解決するため，新しい概念に基づく閉域網(Personal-View SandBox network: PV-SBN)の構成法と，同網を既存 IP 網へオーバーレイする方法を提案する．PV-SBN は通常の VPN とは異なり，個々の端末とアプリケーションごとに定義され，発側端末が送信する IP パケットを，発側端末のプロファイルと着側端末の通信許可条件との照合結果に基づき，ISP 網の入り口でフィルタすることにより，第三者からの着側リソースに対する DoS 攻撃を回避する．さらに，端末によるグローバル IP アドレスの使用を廃止し，新しい概念に基づく IP アドレス(Personal-View SandBox network ID: PV-SBID)を導入する．本概念では同一の着側端末の IP アドレスを発側の個々の端末・アプリケーション毎に独立とすることで，ネットワークレイヤ(IP)での名寄せやなりすましを原理的に不可能とする．PV-SBN は，端末から見ると通常の VPN と等価であり，既存の IP 設備や TCP/IP プロトコルスタックを無改造で活用できる．また，通信毎のシグナリングが不要なため，機能や性能・電力に制限のあるマシン間通信に対しても十分に適用可能である．

キーワード 次世代インターネット， セキュリティ， DOS 攻撃， なりすまし，名寄せ， オーバーレイ，M2M

Dynamic Personal-View SandBox Networks for Next Generation Internet

Takeshi OGAWA† Yuta KOBAYASHI† and Noriharu MIYAHO†

†Tokyo Denki University, School of Information Environment 2-1200 Muzai-gakuendai, Inzai-shi, Chiba, 270-1355 Japan

E-mail: t.ogawa@mail.dendai.ac.jp

Abstract Dos attacks, IP address spoofing and name-based aggregation are important issues to be solved in the Internet. In this paper, a new concept of closed network, called by “Personal-View SandBox network (PV-SVN)”, and its over-laying methods are proposed. Contrary to the existing VPN, a unique PV-SBN is defined for each terminal and application. When a terminal sends a first packet of a flow, the ISP of the sender filters the flow at network ingress gate way based on the matched results of the senders’ profile and the receiver’s access policy. With this mechanism, Dos attack packets against un-allowed receivers cannot enter the Internet. Furthermore, the using of global IP addresses by terminals is abolished, however, a new concept of IP addresses called by “Personal-View SandBox ID (PV-SBID)” is introduced. With the PV-SBID concept, a unique receiver’s IP addresses used by senders are independent, so IP address spoofing and name-based aggregation are never enabled. For a terminal, communication in a PV-SBN is completely same as in a usual VPN, and existing IP equipment and TCP/IP protocol stack can be used in PV-SBNs without any modifications. Existing terminals can immigrate to PV-SBNs step by step. Furthermore, as terminals in PV-SBNs can communicate without specific signaling procedures, it can be applied to M2M communication where hardware resources are extremely limited.

Keywords Next generation internet, Security, DoS attack, Spoofing, name-based aggregation, over lay, M2M

1. はじめに

従来のインターネットでは，端末に対する DoS 攻撃の影響を回避するため，端末と ISP 網の境界あるいは ISP 網内に Firewall(以下 FW)を設置し，着端末に DoS 攻撃パケットを到達させない構成が一般的である．しかしながら，当該 FW にリーチャブルな IP アドレス(グローバル IP アドレス)が通信相手に公開されるため，悪意のある第三者に漏洩すると当該アドレス宛の DoS 攻撃がなされる可能性がある．攻撃トラヒックが着側 FW の性能を超えたり，ISP 網と着側 FW 間のアクセス回線の帯域が占有されると，仮に，着側 FW で当該の攻撃パケットをフィルタした場合でも，通信中断を回避できない状況が生じる．

また，第三者が当該端末になりすました反射攻撃に利用される場合もある．反射攻撃では，当該端末を直接に DoS 攻撃せず，当該端末のグローバル IP アドレスを詐称して，当該端末と通信可能な第三の端末(NTP や DNS など)に短パケットを送信する．第三の端末は多量の応答データを当該端末(FW)に送信する必要が生じ，当該端末や着側 FW への DoS 攻撃が実現する．2014 年には，NTP サーバを使用し，ほぼ 400Gbps の負荷を加える攻撃が実施され，社会

的問題となった[1].

一方，グローバル IP アドレスをキー情報として，ユーザが利用する様々な Web サービスに分散された個人情報を名寄せし，個人が特定される危険性もある.

現状のISPサービスでは，IPアドレス数の不足対策として，一般ユーザの端末に対してはNATやNAPTを適用し，グローバル IP アドレスを長時間に渡り，固定割付しない運用も適用し得る．その結果，名寄せの危険は軽減されるが，FW(NAT/NAPT)に対する DoS 攻撃や DDoS 攻撃の危険性は残存する．さらに，IP レイヤでの着信ができず，発信専用に制限されることとなり，問題と考えている.

本稿では，次世代インターネットに向けて，新しい概念に基づく閉域網(Personal-View SandBox Network: PV-SBN)を既存 IP 網にオーバーレイして構成し，インターネット内の端末間の基本的な通信手段にすることで，上記セキュリティ上の問題に加え，IP アドレス不足，IP レベルの着信不可，等の問題を同時かつスケーラブルに解決する方法について提案する．具体的には，着側端末が提示した通信許可条件に合致した発側端末のみを当該 PV-SBN のメンバ(ホワイトリスト)として ISP 網が管理することにより，攻撃の可能性がある第三者からの着信を原理的に不可能とする．また，端末によるグローバル IP アドレスの使用を廃止し，新たに定義する主観的な IP アドレス(Personal-View SandBox Identifier: PV-SBID)を通信相手の識別子に用いることにより，IP レイヤの名寄せやなりすましを原理的に不可能とし，同時に IP アドレス不足を回避し，IP レイヤの直接通信も実現する.

以下の章では，2 章において次世代インターネットに向けて想定する通信サービスの例を示し，3 章で関連する従来技術と課題を示す．4 章で PV-SBN の構成を，5 章で端末間のデータ通信手順を述べる．6 章で PV-SBN のメンバを ISP に登録する手順に関する要件を述べる．また，7 章で，提案方式のスケーラビリティを確認するため，OpenFlow を用いたプロトタイプ実装により，PV-SBN におけるデータ通信性能と既存 FW 方式の性能との比較結果を述べる．最後に 8 章でまとめを述べる.

2. 想定する通信サービス

本稿ではネットワークレイヤ(IP)において主に以下の 2 種類の通信サービスの実現を想定する．なお，端末やサーバー間では，ftp，sip，rtsp など，既存の NAPT を通過できないアプリケーションは除き，既存の IPv4 上で動作する任意のアプリケーションを対象とする.

(1) **M2P** 通信サービス

本稿では，着端末が不特定のユーザに提供する機能へのリンクを示すurlを公開するとともに，通信を許可する発端末の条件を指定し，ISP がこの条件に合致する不特定多数の発端末からの IP 通信のみ当該着端末に転送するコネクションレス通信サービスを Mult-point To Point (M2P)通信サービスと呼ぶ．通信開始前は，発着端末間で，データ交換を許容できる信頼関係がない，と仮定し，網が着端末に代行して条件の判定を行い，網の入り口で発信パケットのフィルタや発着相互の匿名化を行う.

【例 1】低信頼端末からの着信規制

不特定多数のユーザに Web サーバを公開するが，端末の使用者を特定可能な端末のみに，匿名でのアクセスを許可する．攻撃を検出した場合には，IP アドレスと使用者のリンクをとり，攻撃端末の特定と攻撃の遮断，損害賠償請求等が行える.

【例 2】端末プロファイルによる匿名接続

Web サーバが，端末プロファイル(使用者の年齢，居住地域等)と接続先サーバを指定し，網が端末を匿名で振り分ける.

【例 3】サービス機能の網接続位置の隠蔽

Web サービスを実行している仮想または物理サーバの IP アドレスを，サーバの網内での物理的な位置(location)と独立とし，ASP (Application Service Provider)の構成を攻撃者から隠蔽すると同時に，当該サービスを実行するサーバを変更した場合でも通信相手から変更を隠蔽する.

(2) P2P 通信サービス

本稿では，着端末が特定の発端末に対して IP パケットを用いたコネクションレス通信を許可するサービスを Point To Point (P2P)通信サービスと呼ぶ．通信開始前に，発着端末間で限定された信頼関係が成立していると仮定し，網が着端末に代行して，限定された信頼関係に応じたデータ交換の許可や発着相互の匿名化を行う.

【例 1】端末間サーバレス匿名 IP 通信

共通の趣味・サークル等の限定的な関係があり，ニックネームで SNS などのサーバを介して通信している2者同士が，互

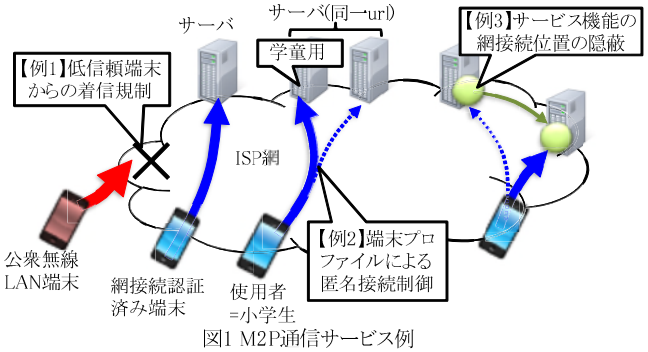


図1 M2P通信サービス例

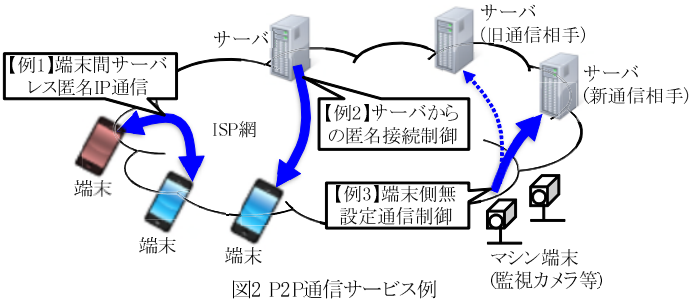


図2 P2P通信サービス例

いに匿名のまま，信頼関係に応じたデータ交換(ビデオホンや，動画共有など)を，SNS などのサーバを介さずにネットワークレイヤで結合した広帯域通信により行う．

【例 2】サーバからの匿名接続制御

ネットショップへの問い合わせ応答や，商品リコール時のユーザへの連絡など，用途や有効期間を限定して Web サーバから端末への IP での直接通信を許可する．

【例 3】マシン端末の持ち主が当該マシンの通信相手や条件（頻度，期間など)を網に登録し，当該マシンへの設定をせずに通信相手の変更などの通信制御を行う．

3. 関連技術と課題

文献[2] では，DoS 攻撃を端末や網が検出すると，送信元の IP アドレスをブラックリストに登録し，ISP 網の入り口で当該リストにある通信を遮断する方法が提案されている．しかしながら，反射攻撃などでは，攻撃の検出や攻撃者の特定に時間がかかり，遮断が間に合わない可能性がある

なお，DoS 攻撃の防止と任意の端末間通信の両立を実現するために，通信時に端末と網間のシグナリングにより着端末が許可した場合に FW(ネットワーク)を通過できるようにするコネクション型の方法がある．IMS[3]では IMS-Gateway や CSCF などのネットワーク装置をシグナリングで制御することで上記を実現する．Skype，WebRTC[4]などでは FW traversal 技術を使用してホーム Gateway などの FW を通過可能なグローバルアドレスを発見することで実現する．ただし，何れも本稿で検討対象とした，着側リソースに対する攻撃について，現状では全く対策なされていない．また，コネクション設定処理自体が着端末への DoS 攻撃となる危険性がある．さらに，Web アクセスのように短いセッションを多数使用するアプリケーションや転送データが少ないマシン間通信では，コネクション設定処理量の比率が高くなる問題もある．

一方，端末アプリケーションの実行時に，他のアプリケーションや OS から隔離されたメモリ領域で動作させることで，当該アプリケーションによるシステムの不正操作や，他アプリケーションによる当該アプリケーションの不正操作を防ぐ SandBox モデルの適用が普及している[5]．ISP が通信用途別に，既存の IP 網にオーバーレイで IP-VPN を構成し，通信を許可する SandBox をメンバ(ホワイトリスト)とすることで，通信毎のシグナリングを実施せずに用途別の閉域性を確保することが期待される．

類似の構成としては，キャリア網内の IP-CUG（Closed User Group)や ISDN-CUG サービス[6]，物理網上に用途別の仮想ネットワーク(SLICE)をオーバーレイする提案[7]が行われている．いずれの方法も，ホワイトリストに基づくメンバ間の通信のみ許可する閉域網をインターネット(または公衆電話網)にオーバーレイするという観点では共通している．しかしながら，2 章で設定した通信サービスを実現するためには，以下の(1)から(4)の技術課題がある．

(1)閉域範囲の最小化

各端末が閉域性を確保すべき通信相手は，同じ用途の通信でも端末間で共通ではなく個々の SandBox 毎に設定がなされる必要がある．例えば，端末 A と端末 B が同一種類の IP 電話アプリケーションを使用して通信する場合，端末 A の IP 電話アプリケーションに通信を許可したい通信相手と，端末 B の IP 電話アプリケーションに通信を許可したい通信相手は，一般に，一部は重なるが他の一部は異なると思われる．仮に，端末 B が端末 A に DDos 攻撃を試みた場合，影響を最小限にするためには，端末 A/B が共通に IP リーチャブルな端末を最小限にする必要がある．すなわち閉域範囲はそれぞれの SandBox 毎に管理できる必要がある．

(2)SandBox 識別子の匿名性

通信相手によるなりすましや名寄せの可能性を排除するためには，各 SandBox はグローバルに当該 SandBox を識別可能な識別子を互いに通信相手に知られずに IP 通信可能とする必要がある．例えば端末 A 内の 1 つの SandBox が，端末 B 及び端末 C 内の SandBox と通信するとした場合，端末 B が認識する端末 A の SandBox の IP アドレスは端末 C が認識するアドレスとは独立で無関係な番号構成とする必要がある．すなわち，VPN で構成される通常の IP ネットワークとは異なり，各 SandBox が自身の番号や通信相手を識別するための IP アドレスは，他の SandBox とは無関係の主観的な番号体系で管理する必要がある．

(3)シグナリングによる通信制御

一般的な IP-VPN や，CUG， SLICE では，閉域網へのメンバの追加・削除は人手による保守作業が必要である．任意の端末間の通信への適用を容易とするためには，端末と ISP 間のシグナリングにより通信許可を行うメンバまたは許可する条件(以下，SBN メンバ条件)の事前登録が必要である．また，発端末が契約する ISP と着端末が契約する ISP は一般には同じ組織とは限らない．着端末が SBN メンバ条件を ISP に登録する時には，両 ISP 間には信頼関係がない場合があり，他 ISP 設備のトランジットが必要な場合も生じ得る．発側の ISP が着側の ISP に代行して発信制御できるように，両 ISP がお互いの信頼性を評価・確認できる仕組みと，ISP 間の通信を MITM(Man in the Middle)攻撃から防ぐ仕組みが同時に必要となる．

(4)次世代インターネットに向けた要件

特に次世代IPでは以下のサービス要件に対する配慮が必要である．

A) 移動透過

IP 端末が移動先で，網との接続点を変更しても，ネットワークレイヤ(IP)より上位に対して，移動状況を隠蔽して通信を可能とする．

B) IP アドレス枯渇への対応

インターネットに接続する IP 端末数は，今後のマシン端末数の増大により，数 100 億～10 兆台に及ぶと予測されている[9]. IPv4 で識別できる端末数は高々40 億(=2^{32})のため，IPv6 への移行が進められている．ところが，既に稼働中の端末のプロトコル変更は困難な場合が多く，特に M2M 通信の場合には，IP アドレス長を長くすることによる無線区間の通信効率低下も懸念される．マシン端末の IP アドレスは下位レイヤ情報等を用いて圧縮する方法が提案されているが，インターネット側の IP アドレスの圧縮は困難である[10].

本稿では，一般端末の IPv6 への移行や無線区間でのアドレス長の圧縮を不要としつつ，任意の端末間でのネットワークレイヤでの直接通信が可能となる特質を有する仕組みを提案する．

C) 既存 IP 網との連続性

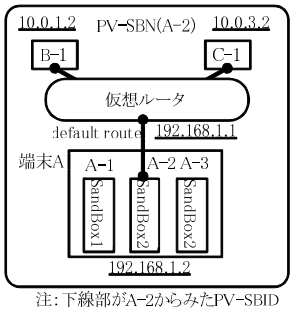
既存インターネットの設備は無駄にせず，有効に活用するために，インターネットや ISP に接続する既存 IP 端末との相互接続も考慮する必要がある．

4. 提案する PV-SBN の構成

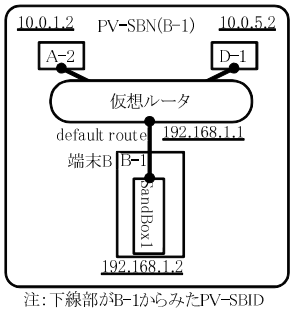
3 章で述べた課題を解決するため，従来の VPN とはリーチャビリティ制御と IP アドレス制御の概念が全く異なる，主観的な閉域網(PV-SBN)を提案する．

本提案では，従来の IP アドレスが担っていた ID (Identifier)とロケータの役割を明確に分離することに特徴がある．端末(Sandbox 内のアプリケーション)から見ると，PV-SBN 内の通信は，通常の IP-VPN 内の通信と等価であり区別出来ず，任意のタイミングで IP によるコネクションレス通信を可能とする．ただし，通信可能な相手端末は，VPN 毎ではなく端末毎に異なり，また IP アドレスによるなりすましや名寄せが原理的にできない．

図 3 に端末 A 内の SandBox(A-2)から見た PV-SBN (A-2)の例を，図 4 に端末 B 内の Sandbox(B-1)から見た PV-SBN (A-2)の例を示す．本稿で新たに導入した用語とその説明を表 1 に示す．



注：下線部がA-2からみたPV-SBID
図3 SandBox(A-2) から見たPV-SBNとPV-SBID



注：下線部がB-1からみたPV-SBID
図4 B-1から見たPV-SBNとPV-SBID

表1 用語の説明

略語	説明
PV-SBN	SandBoxから見た主観的な閉域網
PV-SBID	PV-SBN内でユニークなSandBoxの識別子(IPアドレス)
IV-SBID	ISP網内でユニークなSandBoxの識別子
IV-SBL	IPコア内の転送で用いるIPアドレス
IFID	SandBoxが網に接続するインタフェースの番号

本提案の SandBox は，既存の ios や android におけるアプリケーション sandbox や PC サーバーの仮想マシン，あるいは単用途のマシン端末(1 端末=1SandBox)など，IPv4 の通信が可能で，かつ端末内で互いにメモリやファイルなどが隔離されている任意のアプリケーションを想定している．各端末は，契約する ISP 内で当該端末をユニークに識別できる ID を持ち，ISP に接続時に ISP は当該 ID を用いて接続認証をする，と仮定する．また，ISP は端末ユーザと契約時に入手している個人情報(ユーザの本名，居住地，など)について，匿名で活用の了承をとっている，と仮定する．

各端末は複数の SandBox を同時使用可能とし，ISP は端末毎の SandBox の通番と端末の ID を組み合わせて，ISP 網内で各 SandBox をユニークに識別する番号を IV-SBID(ISP-View SandBox Identifier)として管理する(図 3,4 の A-1,A-2, A-3, B-1, C-1 など)．

SandBox(A-2)から見ると，IP ネットワーク(PV-SBN(A-2))に存在する IP 端末(ユーザのスマートフォン，PC 内のアプリケーション，不特定多数の端末との通信を目的としたサーバ等)は仮想ルータ(192.168.1.1)を挟んで遠方にある B-1 と C-1 のみである．同様に，図 4 に示すように SandBox (B-1)から見ると IP ネットワークに存在する IP 端末は A-2 と D-1 のみである．各 SandBox は自 SandBox と通信相手を各自の PV-SBN の内部で自 SandBox から見てユニークに識別する ID(Personal-View SandBox ID, 以下 PV-SBID)を持ち，通信時には PV-SBID を IP アドレスとして使用し通信相手を指定する．すなわち，1つの Identity である SandBox(例えば A-2)は，ISP が使用する1つの **IV-SBID** (すなわち，A-2)，自 SandBox が使用する1つの PV-SBID，及び通信相手 SandBox が使用する通信相手と同数の PV-SBID を持つ．なお，それらの番号空間は独立である．図 3，図 4 では，ISP 網は全ての SandBox に対して，自端末側の PV-SBID に同一の IP アドレス 192.168.1.2(プライベートアドレス)を静的に配布している．発端末から見ると，着側の SandBox はネットワークアドレス 10.0.x.2(プライベートアドレス)の何れかを固定的に割り振られている．

図 5 に ISP 網の構成と SandBox の接続例を示す．

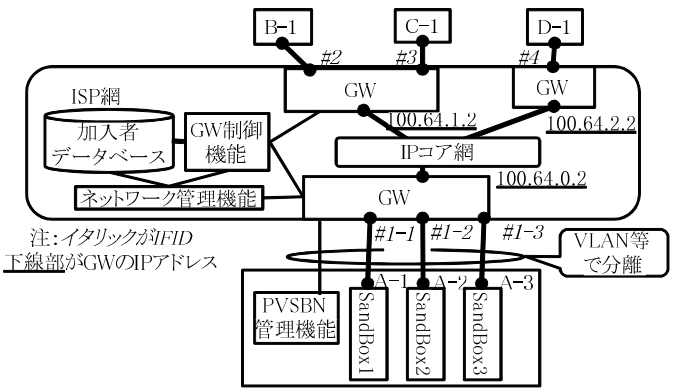


図5　各Sandboxが接続するIFIDとGWのIPアドレス

図 5 の ISP 網が, 図 3, 図 4 における仮想ルータの役割を果たす. ISP は各端末が網に接続するインタフェース点に対して ISP 網内でユニークな ID(以下 **IFID**)を事前に割り当てておく. 端末が網への接続点を変更すると, ISP 網は IV-SBID と IFID の対応を取ることができるため, 移動透過が実現できる. なお, 端末とネットワーク間のリンク上では, 各 PV-SBN は VLAN 等により分離し, SandBox 間の端末内での直接通信は不可とする設定を想定している.

SBN メンバの新規追加や変更を実施したい場合は, 端末の SBN 管理機能部が SBN メンバ条件を網内のネットワーク管理機能部に通知し, 当該機能部が当該条件に一致する発端末を当該 SBN に登録する(6 章参照).

SBN メンバ間でコネクションレス IP 通信実施時の IP パケットのヘッダの変化を図 6 に示す. Gateway (GW)は, 送信元 SandBox が付与した IP パケットの IP アドレス (以下, PV-SBID(S)) を IV-SBID に変換するとともに, 網内のルーティングに使用する locator (ISP-View SandBox Locator, 以下, IV-SBL)すなわち, GW の IP コア網における IP アドレスを宛先及び送信元とする IP パケットにカプセル化して, IP コア網に送信する. IP コア網は既存の IP 方式により IP パケットのルーティングを行う. GW は IP コア網から当該パケットを受信すると, アウターのヘッダを削除し, IV-SBID を受信先 SandBox が理解できる IP アドレス(以下, PV-SBID(R))に再度変換して宛先 SandBox に転送する.変換方法については次項に示す.

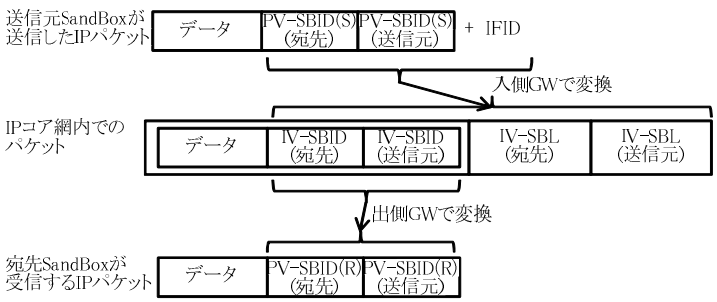


図6 SandBox間通信でのヘッダの変化

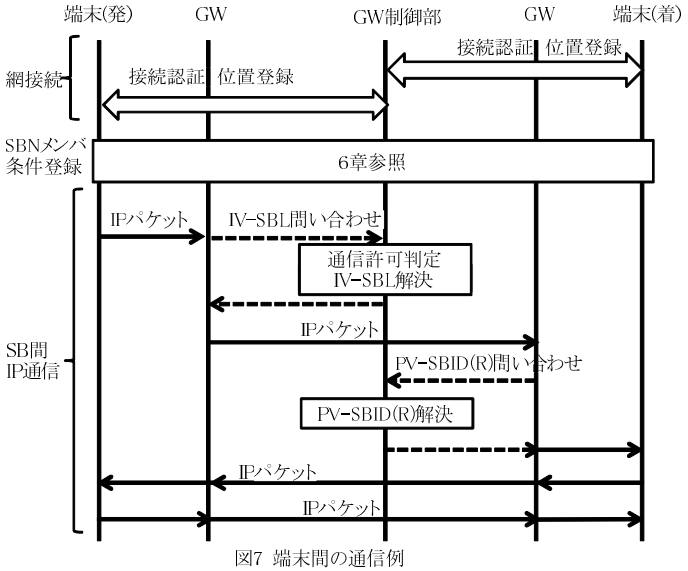


図7 端末間の通信例

各 SandBox が管理する PV-SBID の数は, 実際に通信する通信相手数になるため, 端末における IP アドレスの枯渇問題も回避され, 一般端末の IPv6 への移行やマシンにおけるアドレス長のステートフルな圧縮が不要である.

5. 端末間通信手順

単一 ISP に発着端末が接続する場合の通信例を図 7 に示す. ISP 網内の加入者データベース(以下, DB)で管理するテーブル内容を表 2 と表 3 に示す. 本章では, 事前に着端末が SBN メンバの条件を網に通知し, 網は当該条件に合致する発側の SB を SBN メンバテーブル(表 3)に登録済みであると仮定している. なお, 本テーブルは IV-SBID により分割してスケールアウト可能である. また各端末(Sandbox)の網内の位置を記録する位置管理テーブル(表2)も, IV-SBID 及び網への接続位置で分割しスケールアウト可能である. 提案する通信処理手順を以下に示す.

1) 網は端末と接続認証を完了すると, 接続インタフェース点番号(IFID)および IV-SBL と, 当該端末の IV-SBID との対応を, DB 内の位置管理テーブル(表 2)に記録する. 端末の ID は ISP と契約時に, IV-SBID は後述の SBN メンバ登録手順で決定する.
2) SandBox(A-2)が C-1 宛のパケットを, 網との接続認証後に初めて送信した場合は, GW は当該パケットのヘッダ情報(PV-SBID)と IFID を制御部に転送し, 変換後の IV-SBL を問合わせる.
3) 制御部は, IV-SBL(送信元)と IV-SBID(送信元)を IFID から前述の位置管理テーブルを活用して決定する. IV-SBL(宛先)と IV-SBID(宛先)は, 以下の2段階で決定する. まず, 通信可能な SandBox の IV-SBID とそれぞれの視点による発着 SandBox の PV-SBID との対応を管理する SBN メンバテーブル(表 3)を IV-SBID(送信元)と PV-SBID(宛先)の2つをキー

表2 位置管理テーブル

位置管理テーブル(正引き用)

IFID	IV-SBL	IV-SBID
#1-1	100.64.0.2	A-1
#1-2	100.64.0.2	A-2
#1-3	100.64.0.2	A-3
#2	100.64.1.2	B-1
#3	100.64.1.2	C-1
#4	100.64.2.2	D-1

位置管理テーブル(逆引き用)

IV-SBID	IFID	IV-SBL
A-1	#1-1	100.64.0.2
A-2	#1-2	100.64.0.2
A-3	#1-3	100.64.0.2
B-1	#2	100.64.1.2
C-1	#3	100.64.1.2
D-1	#4	100.64.2.2

表3 SBNメンバテーブル

発側			着側		
IV-SBID	SV-SBID(S) (送信元)	SV-SBID(S) (宛先)	IV-SBID	SV-SBID(R) (送信元)	SV-SBID(R) (宛先)
A-1	192.168.1.2	10.0.1.2	B-1	192.168.1.2	10.0.1.2
A-1	192.168.1.2	10.0.3.2	C-1	192.168.1.2	10.0.1.2
B-1	192.168.1.2	10.0.1.2	A-1	192.168.1.2	10.0.1.2
C-1	192.168.1.2	10.0.1.2	A-1	192.168.1.2	10.0.3.2

にして検索し，着側の IV-SBID(宛先)を決定する．さらに，位置管理テーブルを活用しIV-SBL(宛先)を決定する．次に，決定した IV-SBL(送信元/宛先)と IV-SBID(送信元/宛先)を GW に返答する．

4) GW は C-1 宛パケットの IP アドレスを，指示された IV-SBL 及び IV-SBID に変換してルータに転送する．
5) ISP 網内では，既存の IP ルーティングにより，IV-SBL(宛先)に該当する GW まで転送する．
6) 着側 GW は，初めて A-2 から C-1 宛(IV-SBL)の IP パケットを受信した場合，当該パケットの変換後の PV-SBID を制御部に問合わせる．
7) 制御部は，IV-SBID をキーにして位置管理テーブルを逆引きし，C-1 の接続する IFID を決定する．また SBN メンバテーブルを検索し，端末 C の認識する PV-SBID を決定する．次に，決定した IFID(パケットの転送先)と PV-SBID を GW に返答する．
8) GW は端末 C 宛パケットの IP アドレスを，指示された PV-SBID に変換し，指示された IFID に転送する．通常の NAT/NAPT による FireWall では，クライアントの IP アドレスとポート番号のみ変換し，アドレスプール中の未使用の IP アドレスを動的に割り当てるが，本提案の GW では宛先及び送信元 IP アドレスの双方を変換し，SBN メンバテーブルに記録されているアドレスを静的に割り当てる．

一旦，SBN メンバが網に登録されれば，各 SandBox は ISP 網を介して，登録された任意のメンバ(SandBox)と IP レイヤで直接通信ができる．各 SandBox 内通信ソフトは，信頼関係のない SandBox からの着信や NAT の存在を意識することは不要である．従って SIP などのセッション制御プロトコルや WebRTC などの FW トラバーサルソフトの実装が不要となり，閉域網内と同様な IP レイヤのみによる直接通信を考慮すればよい．

6. SBN メンバ登録手順

5 章で述べたデータ転送手順を前提とすると，SBN メンバの登録手順は以下の要件を満たす必要がある．これら要件を満たす手順及びそのスケーラビリティについては，別途報告する．

(1) M2P 通信サービス

本サービスでは，着端末が SBN メンバ条件(メンバ加入を許可する条件)を ISP に通知時に発端末を特定しない．このため，発側の ISP も不特定となる．従って，着端末が提供する機能の url に加えて当該機能に対する SBN メンバ条件を，インターネットに接続する全 ISP に伝搬させる仕組みが必要である．また，着端末が SBN メンバ条件の通知を完了しても，ISP は発端末を特定できないため，発端末の SBN メンバテーブルを更新できない．このため，発端末が最初に当該 url から宛先 IP アドレスを解決時に，発端末の属性と，当該条件を比較し，適合した場合にのみ，PV-SBID(S)を網が払い出し，SBN メンバテーブルを更新することが必要である．

(2) P2P 通信サービス

本サービスでは，着端末が SBN メンバ条件を ISP に登録時に，発端末を特定する必要がある．しかしながら発着端末は，自端末をグローバルに識別可能な情報を相手端末に知られてはならない．ただし，ISP は接続を許可する両端末をユニークに識別可能な情報(IV-SBID)を入手できる必要がある．また，登録手順を相手端末に対する DoS 攻撃に悪用できないことが，手順上保証されている必要がある．

なお，SBN メンバ条件に，M2P 通信と同様に許可条件を追加することで，発端末がオープンにしている個人情報(性別，居住地，場合によっては本名など)の信頼性を ISP が判定し，着信を制御することも可能とする．

7. SB 間 IP 通信の基礎性能評価

提案方式は，従来技術による FW(NAPT)と比較すると，ヘッダ変換ルールが複雑であり，また，トンネル処理が必須である．このため，提案方式のスケーラビリティ確認を目的として，提案方式と，従来技術による FW(NAPT)の基本機能の双方を実装し，GW と制御部の性能比較を行った．実装には，既存の OpenFlow 制御ソフトである Trema と，OpenvSwitch を組み合わせて使用した．評価網の構成を図 8 に，装置仕様と測定条件を表 4 に示す．

NAPT については，GW は，発側 SandBox が送信する IP パケットの発着 IP アドレスと UDP ポート番号でフローを識別し，新規フローを検出すると制御部に通知する．制御部はポート番号プールから，過去に当該フローに割り当て済みのポート番号またはどのフローにも割り当てられていない番号を検索して GW に通知する．以後は，当該フローについ

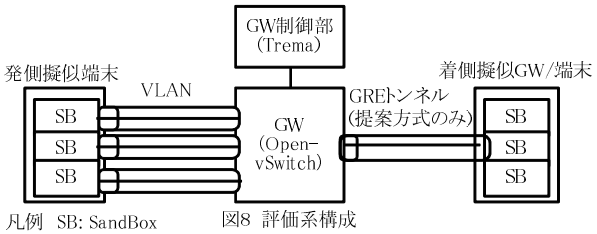


図8 評価系構成

表4 装置構成と評価条件

ハードウェア	HP ProLiant MicroServer,AMD Turion II NEO N54L(2.2 GHz),メモ4GB,HD 500GB, GbE
ソフトウェア	Ubuntu DeskTop 14.04, IPv4, Trema 0.4.6, OpenvSwitch 2.0.2, pktgen 2.7.4
通信形態	発側SB(VLANID)をランダムに変化させてパケットを生起，宛先は固定(1:1).逆方向のパケット送信はなし.
SB数	発側SB, 着側SB共に4095(実際は1台のサーバ内のpktgenで擬似)
IPパケット	UDP, L2ヘッダを含めて100B固定
測定方法	発側でpktgenのパケット送信間隔(固定値)を指定し，一定個数のパケットを送信. 送信数は，25pps以下では1,000パケットそれ以外では10万パケット. 着側でtcpdumpにより到着数と到着時刻を測定

ては GW 内のフローの制御ルールに基づいてヘッダ変換する実装を行った. なお, アドレスプールはハッシュテーブルで構成し, 繰り返し検索(ruby の find メソッドと each メソッド)を使用した.

提案方式の処理メカニズムは, 4 章・5 章で述べた通りである. 提案方式では NAPT と異なり, 端末が通信を開始する前にヘッダ変換後の発着アドレスが確定している. このため未割り当てポート番号の検索は不要である. また GW 間のトンネルについては, OpenvSwitch の機能を用いて GW と着側の擬似端末間に 1 本の GRE(Generic Routing Encapsulation)トンネルを設定して擬似している.

(1) GW の性能評価

提案方式の場合, フロールール数は発着 SandBox のペア数×2(双方向), NAPT の場合フロールール数は発着 SandBox のペア数×2×トランスポート層の多重数, となる. 本評価では基礎評価としてトランスポート層の多重数=1(固定)とし, 両方式とも SandBox4,095 個×双方向=8,190 を, GW 内の OpnevSwitch に有効期間無限大で登録した. そして, 各方式の性能限界を比較するため, 発側擬似端末からのパケット送信間隔を 15μs～2.6μs に変化させて UDP パケットを GW へ入力し, GW から出力されたパケットの送信レートを測定した(GW への入力レートは 67kpps～380kpps). また, 提案方式における GRE トンネルの影響を見るため, 提案方式で GRE トンネルを設定しない場合についても測定した. 入力レートに対する出力レートのレート比を図 9 に示す. 入力レートの最大値 380kpps は, 試験環境で擬似端末が送信できる最大レートである. 例えば, 提案方式で入力レートが 380kpps の場合, 出力レートは 63.1kpps(レート比 16.6%)となった.

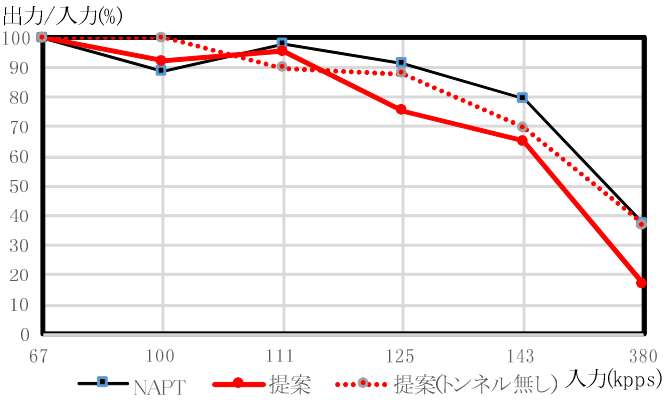


図 9 GW性能測定結果

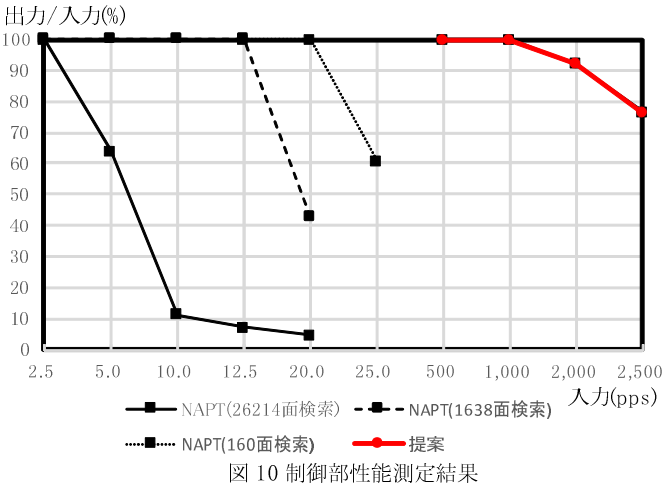


図 10 制御部性能測定結果

提案方式を従来の NAPT と比較すると, 出力が約 20%低い. ただしトンネル無しでは従来の NAPT に近い出力となった. OpenvSwitch のヘッダ変換動作については, 両方式で大きな差はない. またフロールールの数も本評価では同一である. このため GRE トンネルの有無が提案方式の出力低下の主要因と想定できる.

(2)制御部の性能

各方式の性能限界を比較するため, GW 内のフロールールを全て削除し, 発側擬似端末からのパケット送信間隔を 500ms～500μs に変化させて, UDP パケットを GW へ入力し, GWからの出力レートを測定した(GW への入力は 2.5pps～2,500pps). なお, フロールールの有効期間は最小値(1 秒)とした. 本測定では GW からの出力レート(制御部から GW へのフロールール設定レートと同等)を制御部の性能とみなしている. NAPT については 1 個の IP アドレスの 65 万個(2^{16})個のポートを全 SB で共有した. また未使用ポート番号検索処理の影響を評価するため, 使用中ポート数(未使用のポート番号を発見するまでにサーチする回数)を 26,214(65 万個の 40%), 1,638(2.5%)及び 160(0.25%)の3パターンで測定を行った. 入力レートに対する出力レートの比を図 10 に示す.

提案方式を従来の NAPT と比較すると, 使用中ポート数が 160 の場合と比較し 50 倍(1,000/20), 26,214 の場合と比較し 400 倍(1,000/2.5)程度, 提案方式の出力が向上することが判明した.

従来方式と大きな差が生じた理由は, NAPT でのポート番号検索を, 単純な繰り返し検索としたことが主要因と考えられる. このため, 検索アルゴリズムの工夫により, NAPT での性能は向上する可能性がある.

8. おわりに

本稿では, 次世代 ISP 網の実現に向けて, 従来から知られている IP アドレス数枯渇問題などに加え, 悪意端末からの攻撃と, 名寄せ・なりすましを同時に解決する, 主観的な IP 閉域網(PV-SBN)の構成と, 同網を既存 IP 網へオーバーレイする方法を提案した.

本方式は, 着端末が事前に示した通信許可条件に適合する発端末に対して, 原理的になりすまし・名寄せができない IP アドレスを用いた, 端末間の匿名による IP レイヤ直接通信を実現できる特徴を有する. PV-SBN のメンバ間では, 通信毎のシグナリングが不要であり, また IP アドレス長の拡大が不要なため, 特に機能や性能・電力に制限のあるマシ

ン端末間の通信では，大きなメリットがあると考えられる．また，提案方式と既存のFireWall(NAPT)方式をOpenFlowにより実装し，GW については 20%程度性能が低下するものの，制御部の処理性能については，同等以上の性能が発揮できることを示した．

今後は，次世代インターネットへの適用を目的として，SBNメンバ登録手順，ISP網の相互接続方法，及びトランジット網を介した接続方法について検討を進める予定である．本稿は電子情報通信学会研究会の発表[11]を元に，サービス具体例の追記と，評価結果の追記を行ったものであることを申し添える．

文　献

[1] 日本ネットワークインフォメーションセンタ,https://www.nic.ad.jp/ja/materials/iw/2014/proceedings/s8/, 2015.8.7 閲覧

[2] 岡田康義,他,"セキュリティポリシーに基づくネットワークトラヒック制御の提案," 情報システム学会誌,Vol.9,No.2,2014 年 3 月,

[3] Technical Specification Group Services and System Aspects (2006), IP Multimedia Subsystem (IMS), Stage 2, V5.15.0, TS 23.228, 3GPP, 2006

[4] WebRTC,http://www.webrtc.org/, 2015.8.7 閲覧

[5] 可児潤也，他．"SaaR: Sandbox as a Request の実装と評価." 情報処理学会研究報告．マルチメディア通信と分散処理研究会報告 2014.19

[6] "Integrated Services Digital Network (ISDN);Closed User Group (CUG) supplementary service, Service description," ETS 300 136

[7] 鈴木一哉，他．"OpenFlow 技術とその応用." コンピュータ ソフトウェア 30.2 (2013): 2_3-2_13.

[8] Alliance, N. G. M. N. "5G White Paper-Executive Version." White Paper, December (2014).

[9] "2020 年に IoT(Internet of Things)の普及でつながるデバイスと市場の成長性.", http://blogs.itmedia.co.jp/business20/2014/06/2020iotinternet-c56b.html, 2015.8.7 閲覧

[10] J. Hui et al, "Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks," RFC 6282, 2011. 2015.8.7 閲覧

[11] 小川猛志,他," Dos 攻撃・なりすまし・名寄を防ぐ動的な匿名閉域通信方式の検討" 電子情報通信学会技術研究報告. 2015 年 9 月発表予定