IIR

Internet
Infrastructure
Review

Dec.2017
Vol.37

定期観測レポート

IIJインフラから見るインターネットの傾向

フォーカス・リサーチ(1)

VSSはユーザデータを守らない

フォーカス・リサーチ(2)

商用化を迎えたVideo over IP技術とその経済圏

フォーカス・リサーチ(3)

Intent-Based Network Security

IIJ
Internet Initiative Japan

Internet Infrastructure Review

December 2017 Vol.37

《 読者アンケート 協力のお願い 》

今号をお読みいただいたご意見・ご感想をお聞かせください。今後の参考にさせていただきます。
回答いただいた方の中から抽選で30名様にインターネット便利帳付きIIJオリジナルリングノートをプレゼントいたします。
※なお、当選のお知らせは、プレゼントの発送をもってかえさせていただきます。

【 アンケート受付期間 】
2017年3月30日（金）まで

【 回答方法 】
IIJのWebサイト内、以下のページまたは右側のQRコードからご回答ください。
（https://biz.iij.jp/public/application/add/437）

エグゼクティブサマリ

前号でお知らせしましたように、IIRではコンテンツの見直しを行っており、この37号は見直し後の第2号となります。35号まで定期的に掲載しておりましたインターネットセキュリティのサマリーにつきましては、wizSafe Security SignalというWebサイトでIIJのSOCチームから月次で観測レポートを出すことになりました。9月分から掲載されており、よりタイムリーな情報発信に努めて参りますので、そちらもぜひご覧ください。

IIRはIIJで研究・開発している幅広い技術のご紹介を目指しており、私たちが日々のサービス運用から得られる各種データをまとめた「定期観測レポート」と、特定テーマを掘り下げた「フォーカス・リサーチ」から構成されています。

1章では、今号の定期観測レポートとして、IIJのネットワーク・サーバインフラを運用するなかで得られる情報をもとに、BGPの経路、DNSのクエリ、IPv6のトラフィック、モバイルのトラフィックなど、インターネットの現状を見つめてみました。これらの情報をIIRでご紹介するのは初めてで、まだ現時点の途中経過しかご報告できないものもありますが、今後は定期的にご紹介していく予定です。

2章から4章はフォーカス・リサーチです。2章ではWindowsに搭載されているバックアップ関連の機能であるVSS（Volume Shadow Copy Service）を取り上げました。VSSはスナップショットを作成することができ、攻撃者が使用した攻撃ツール、一時ファイル、改ざんされたファイルなどの復元に利用できるため、デジタルフォレンジックにおいて非常に重要なデータの1つとして認識されていますが、デジタルフォレンジックの技術調査を行うなかで、VSS を有効にしていてもユーザデータがスナップショットに正常に保存されない事象を確認しました。その原因と影響範囲、更には対処方法についてご紹介します。

3章は、放送局でも急速に関心と期待が高まっているVideo over IP技術についてです。インターネットの普及と共に、様々なメディアがIP（Internet Protocol）をインフラとして用いるようになりました。雑誌・新聞や、CD・DVDで配信されていた音楽や映像のコンテンツなどもIP上で配信されています。今、注目されているのは、放送局で扱うような圧縮されていない音声・映像信号をIPネットワークで扱おうというものです。本章ではVideo over IPが必要とされる背景や、規格化の状況、IIJで行っているPoC（Proof of Concept）の活動についてご紹介します。

4章では、SDN、SD-WANの次と言われているIntent-Based Networking（IBN）を取り上げました。IBNにおいて、ユーザは業務的に実現したいポリシーを規定し、ネットワークがその実現可能性を検証して、自動でそのポリシーを実現します。そして、ネットワークはその状態を常時監視し、それを維持・最適化します。IIJではゼロ・トラスト環境を前提としたセキュリティの新しい仕組みをIBNで実現しようとしています。本章では、その取り組みの具体的な内容や、今後の展望についてご紹介します。

IIJでは、こうした活動を通じて、インターネットの安定性を維持しながら、日々改善・発展させていく努力を行っています。今後も、お客さまの企業活動のインフラとして最大限に活用していただけるよう、様々なサービス及びソリューションを提供し続けて参ります。

島上 純一（しまがみ じゅんいち）
IIJ 取締役 CTO。インターネットに魅かれて、1996年9月にIIJ入社。IIJが主導したアジア域内ネットワークA-BoneやIIJのバックボーンネットワークの設計、構築に従事した後、IIJのネットワークサービスを統括。2015年よりCTOとしてネットワーク、クラウド、セキュリティなど技術全般を統括。2017年4月にテレコムサービス協会MVNO委員会の委員長に就任。

IIJインフラから見るインターネットの傾向

IIJではインターネットサービスを提供するために、国内でも有数規模のネットワーク・サーバインフラを運用しています。ここでは、IIJのインフラ運用を通じて得られた情報を元に、現在のインターネットがどのような傾向を持っているのかを検討し、紹介します。

取り上げるテーマは、ネットワークの経路情報、DNS問い合わせ情報、IPv6利用状況、モバイル接続サービス利用状況です。また、IIJのトラフィックの大部分を支えるバックボーンネットワークの現状についてもあわせて報告します。

Theme 01

BGP・経路数

2011年2月3日に全世界のIPアドレス資源を管理するIANAのIPv4アドレス在庫が枯渇してから約6年半が経過しました。現在では、IANAからIPアドレスの割り振りを受け、各国に割り振りを行う世界5つのRIRすべてが最後の/8ブロックからのアドレス割り振り・割り当てを開始(または既に終了)している状況にあります。一方、インターネットで観測される、いわゆるIPv4「フルルート」数はIANAアドレスの枯渇後も順調に増加を続けており、現在では2011年当時の約2倍に達しようとしています。本節では弊社網から他組織に広報しているIPv4「フルルート」(相当)の情報を基に経路数の推移などを改めて確認します(表-1、図-1)。

総じてプレフィクスが長い経路で増加率が高い傾向にあるのは予想どおりと言えます。中でも/22経路の増加が目立ちますが、これは最後の/8ブロックが残り少ないRIRからのIPv4アドレス割り振り・割り当てサイズが(最大)/22(1024アドレス)に制限されている影響と考えられます。

また/8経路数が減少している一方でその他は満遍なく増加していることも分かりますが、これはアドレス移転を目的としたアドレスブロック分割の影響が現れているのではないかと思われます。アドレスブロックの分割が発生すると、簡単に言えば表-1

表-1「フルルート」に含まれるプレフィクス長ごとのIPv4経路数の推移

年月	/8	/9	/10	/11	/12	/13	/14	/15	/16	/17	/18	/19	/20	/21	/22	/23	/24	total
2010年9月	20	10	25	67	198	409	718	1308	11225	5389	9225	18532	23267	23380	30451	29811	170701	324736
2011年9月	19	12	27	81	233	457	794	1407	11909	5907	9885	19515	26476	26588	35515	34061	190276	363162
2012年9月	19	14	29	84	236	471	838	1526	12334	6349	10710	20927	30049	31793	42007	39517	219343	416246
2013年9月	16	11	30	93	250	480	903	1613	12748	6652	10971	22588	32202	34900	48915	42440	244822	459634
2014年9月	16	12	30	90	261	500	983	1702	13009	7013	11659	24527	35175	37560	54065	47372	268660	502634
2015年9月	18	13	36	96	261	500	999	1731	12863	7190	12317	25485	35904	38572	60900	52904	301381	551170
2016年9月	16	13	36	101	267	515	1050	1767	13106	7782	12917	25229	38459	40066	67270	58965	335884	603443
2017年9月	15	13	36	104	284	552	1047	1861	13391	7619	13385	24672	38704	41630	78779	64549	367474	654115
増加率(※)	0.75	1.3	1.44	1.552	1.434	1.35	1.458	1.423	1.193	1.414	1.451	1.331	1.663	1.781	2.587	2.165	2.153	2.014

※2010年9月時点を1とした2017年9月時点の値

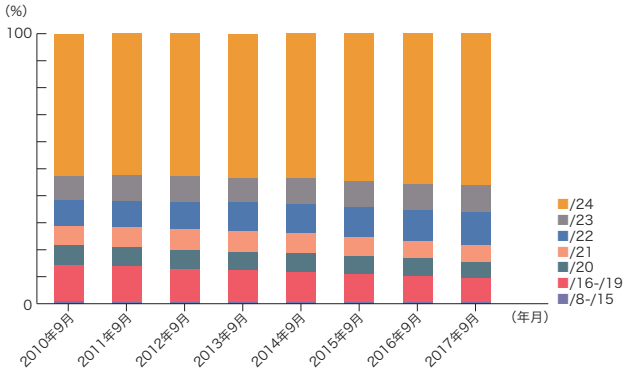

図-1 IPv4「フルルート」に占める各プレフィクス長経路数の比率の推移

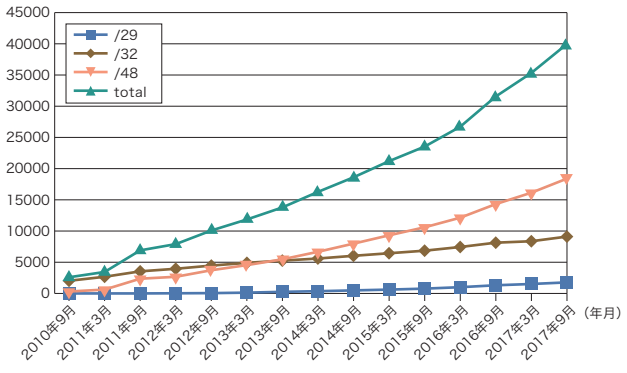

図-2 IPv6「フルルート」数推移

左側の経路数が減少し、同右側の経路数が増加します。アドレス移転は、IPv4アドレス入手の貴重な手段として今後も利用が見込まれるため、IPv4経路数の分布も表-1右側（プレフィクスがより長い方）への偏りが今後更に進むと推測されます。

最後にIPv4の後継となるIPv6の「フルルート」数にも軽く触れておきます（図-2）。IPv4と比べると数はまだ微々たるものですが順調に増加しており、また2016年頃からはその増加の傾きが大きくなっているようにも見えます。各RIRのIPv4アドレス在庫がますます枯渇していく状況下で、地域や組織におけるIPv6対応は今後更に加速していくと推察されます。この傾きがどのように変化するのか、今後が注目されます。

Theme 02

DNS

IIJではインターネット接続サービス利用者がDNSの名前解決を利用できるようフルリゾルバを提供しています。この項では名前解決の情況を解説し、IIJで2017年5月17日に行ったフルリゾルバの1日分の観測データから、主にブロードバンド向けに提供しているサーバのデータに基づいて分析と考察を行います。

フルリゾルバはrootと呼ばれる最上位のゾーン情報を提供する権威ネームサーバのIPアドレスのみを知っており、そこから得られる情報を手がかりに情報を保持しているであろう権威ネームサーバをたどって必要なレコードを探します。フルリゾルバで毎回反復問い合わせを行っていると負荷や遅延が問題となるため、得られたレコードはしばらくキャッシュしておいて再び同じ問い合わせを受けた場合にはそのキャッシュから応答しています。最近はこの他にもブロードバンドルータやファイアウォールなど、通信経路上の機器にもDNS関連の機能が実装されており、DNS問い合わせの中継や制御ポリシーの適用に関わっている場合があります。

ブロードバンド接続やモバイル接続ではPPPやDHCP、RA、PCOなどを利用してフルリゾルバのIPアドレスを利用者に伝えることができます。ISPはこれら機能を利用して、利用者の通信に必要な名前解決用のフルリゾルバを自動設定できるようにしています。ISPは複数のフルリゾルバを利用者に伝えるほか、利用者は自身で設定を変更して利用するフルリゾルバを指定、追加することもできます。端末に複数のフルリゾルバが設定されている場合、どれを利用するかは端末の実装やアプリケーションに依存するため、フルリゾルバ側では利用者が総量としてどの程度の問い合わせを行っているか分かりません。このため、フルリゾルバでは問い合わせ動向を注視しながら、常に処理能力に余裕を持たせた運用が必要となります。

IIJが提供するフルリゾルバの観測データで利用者の動向を見てみると、問い合わせ元IPアドレス当たり1日平均して、0.08query/sec程度を観測しています。この値は利用者の利用動向を示すように時間帯によって変動し、朝4時頃に最小の0.04query/sec、夜9時頃にピークを迎えて0.13query/sec程度になっています。問い合わせの通信に利用されるIPプロトコルにはIPv6とIPv4がありますが、IPv6での問い合わせの方が時間帯による変動が少し大きく見える程度で、ほぼ同じ傾向を示しています。これらの値はここ数年特に変化がなく、0.06ポイント程度の変動範囲に収まっています。変動要素としてクライアントが利用可能なフルリゾルバ数や利用者環境内でのキャッシュ機能、端末やアプリケーションの挙動などが考えられるため、今後の動向の予想が難しく引き続き注視が必要です。

問い合わせレコードタイプに注目すると、ホスト名に対応するIPv4アドレスを問い合わせるAレコードとIPv6アドレスを問い合わせるAAAAレコードがほとんどを占めています。傾向は問い合わせの通信に利用されるIPプロトコルで違いが見られ、IPv6での問い合わせではより多くのAAAAレコード問い合わせが見られます。IPv4での問い合わせでは、全体の64%程度がAレコード問い合わせ、33%程度がAAAAレコード問い合わせです（図-3）。一方IPv6での問い合わせでは、全体の56%程度がAレコード問い合わせ、43%程度がAAAAレコード問い合わせとAAAAレコード問い合わせの比率が高まっています（図-4）。また問い合わせ元のIPアドレスごとに傾向を見ると、IPv4/IPv6での問い合わせにかかわらず、96%程度の問い合わせ元が多少なりともAレコードを検索しています。AAAAレコードに関してはIPv4で57%程度、IPv6で80%程度の問い合わせ元が検索しています。IPv4での問い合わせに占めるレコード比率はここ数年あまり変わらなくなってきているため、近年の新しい実装はIPv6での問い合わせを優先的に利用しているのではないかと推測しています。

Theme 03

IPv6

2011年2月3日、アジアパシフィック地域のIPアドレス資源を管理するRIRであるAPNICのIPv4アドレス在庫がなくなり、日本でも通常のIPv4アドレスの新規割り振り（地域管理組織やISPへの分配）が終了しました。いわゆるIPv4アドレスの枯渇です。それから約6年半が経過しましたが、後継と言われるIPv6を利用したインターネットが爆発的に普及しているかというと、そうではありません。

今回は、IIJにおけるIPv6の利用者数やトラフィック、利用プロトコルの解析を行い、現在の状況を解説します。

■ 利用者数

IIJでは、2011年6月より、NTT東日本及びNTT西日本のフレッツ光ネクストをご利用のお客様にIPv6 PPPoE接続の提供を開始しました。また2011年7月より、IPv6 IPoE接続の提供（関連会社であるインターネットマルチフィード株式会社と共同で提供）を開始しました。2015年7月からは、NTT東西がレンタル提供しているホームゲートウェイからのIPv6 PPPoE自動接続にも対応し、お客様が特に設定を行わなくてもIPv6接続が利用できるようになりました。また、モバイルサービスにおいても、2012年5月の4G（LTE）接続提供開始当初よりIPv6接続に対応しており、端末機器がIPv6対応していれば、モバイルでのIPv6接続の利用も可能です。

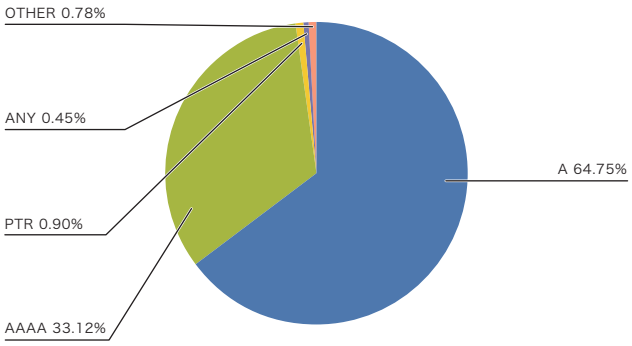

図-3 クライアントからのIPv4による問い合わせ

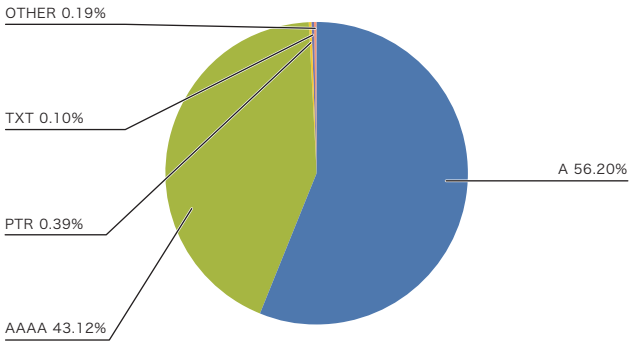

図-4 クライアントからのIPv6による問い合わせ

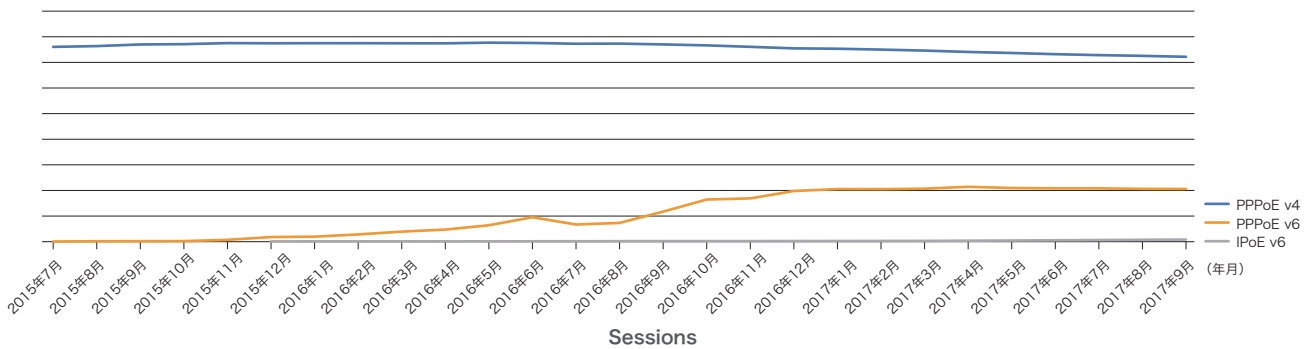

図-5 2015年7月から2017年9月末までのフレッツ光ネクストにおけるIPv4接続数とIPv6接続数の推移

図-5は、2015年7月から2017年9月末までのフレッツ光ネクストにおけるIPv4接続数とIPv6接続数の推移です。IPv4は微減、IPv6は微増となっており、2017年9月時点で、IPv6は全体の22.9%程度(PPPoE 22%, IPoE 0.9%)です。

IPv6利用者数が22.9%程度に留まっているのには、IPv6 PPPoE自動接続に対応していない機器の利用者と、IPv6を提供していない法人契約が一定数含まれるためと考えられ、今後はIPv6 PPPoEについては大きな増加はないと思われます。IPv6 IPoEは現時点では低い水準ですが、DS-Liteを用いたIPv6 IPoEへの移行が少しづつ進んでいくと予想しており、差は縮小していくと考えています。

■ トラフィック

IIJのコアPOP(東京・大阪・名古屋)のバックボーンルータで計測した、IPv4トラフィックとIPv6トラフィックを図-6に示します。IPv4もIPv6も右肩上がりで増加しているのですが、IPv6トラフィックは全体の4%程度にとどまり、IPv4と並べると、潰れて見えなくなるほどで、普及が進んでいるとは言い難い状況となっています。

次に2016年10月から2017年9月までの1年間の平均IPv6トラフィック送信元組織(BGPのAS番号)の上位を図-7に示します。

サービスのIPv6対応を積極的に進めているA社が最上位となっており、2位以降はA社の1/16以下となっています。

IPv4(図-8)においても、1位はやはりA社ですが、2位以降はクラウド大手のD社、CDN大手G社、CDN大手K社と続いており、IPv6との顔ぶれの違いが興味深いところです。また、A社と2位との比率は約1/2となっており、こちらもIPv6とは異なるところです。

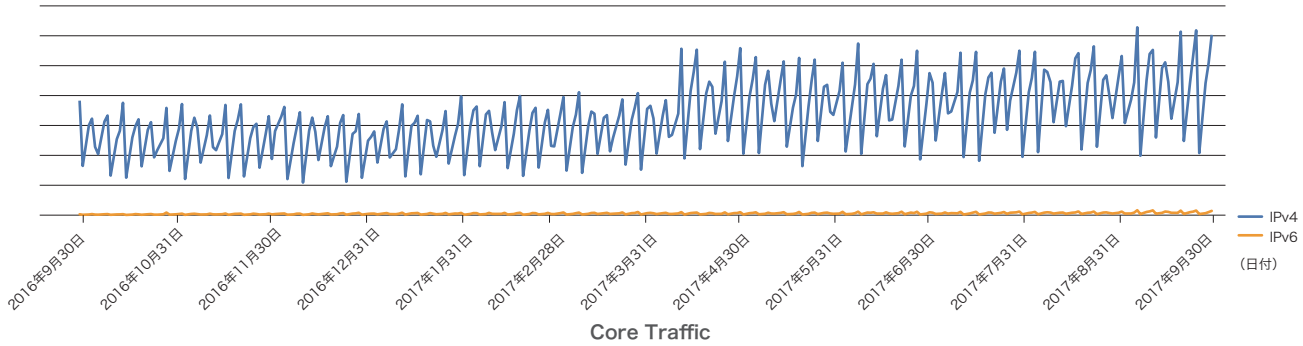

図-6 IIJのコアPOP(東京・大阪・名古屋)のバックボーンルータで計測した、IPv4トラフィックとIPv6トラフィック

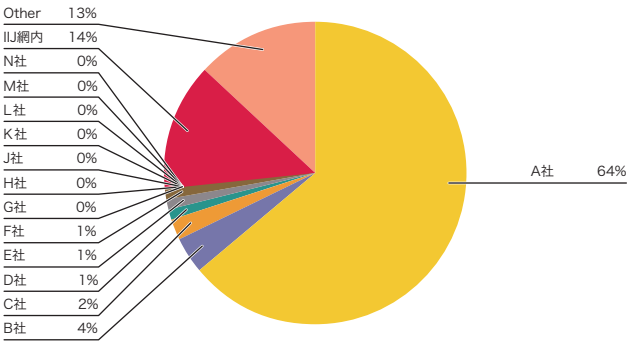

図-7 2016年10月から2017年9月までの
1年間の平均IPv6トラフィック送信元組織(BGPのAS番号)の上位

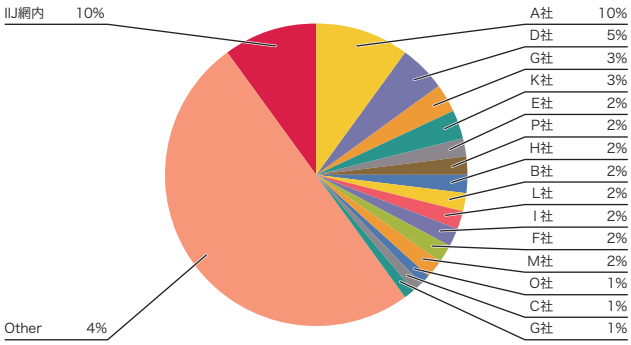

図-8 2016年10月から2017年9月までの
1年間の平均IPv4トラフィック送信元組織(BGPのAS番号)の上位

A社と2位以下のトラフィック量の差をみると、A社以外の事業者はIPv6でサービスを提供しているものの、利用は一部にとどまっているのではないかと推測されます。

■ 利用プロトコル

IPv6トラフィックのProtocol番号（Next-Header）と送信元ポート番号で解析したグラフを図-9に示します（2017-10-01からの1週間）。

約4割が443/TCP（HTTPS）となっており、2位の443/UDP（QUICと思われる）と合わせると5割を超えます。3位が80/TCP（HTTP）ですが、1位2位の1/6程度の量となっており、同期間のIPv4グラフ（図-10）と比べるとその差が顕著になっています。

IPv6の方がHTTPS/QUICの割合が多いのは、A社のトラフィックの割合が多いからだと考えられますが、他の事業者においてもIPv6に対応するような新しいサービスは、当初よりHTTPSでのサービス提供を行っているという一面もあるかもしれません。

■ まとめ

今回はIIJのIPv6の状況について、利用者数・トラフィック量・利用プロトコルを見てみました。IPv6接続環境はそれなりに整備が進んできましたが、サービス事業者側の対応は1社を除きまだ始まったばかりという印象です。今年はモバイルのIPv6対応がいよいよ本格的に始まったこともあり、今後サービス事業者の対応が加速することが期待されます。引き続き様々な観点から分析を進めます。

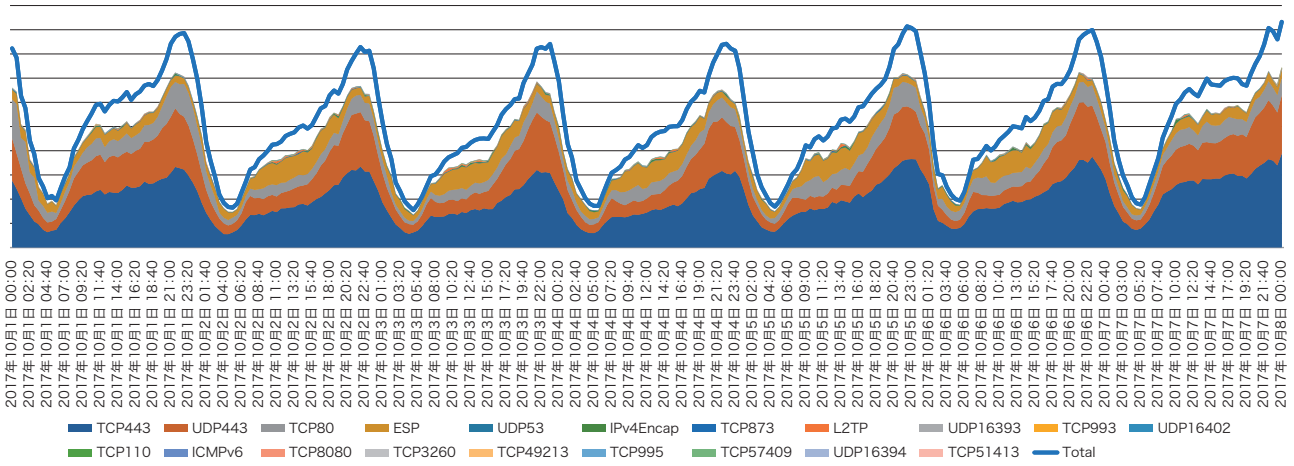

図-9 IPv6トラフィックのProtocol番号（Next-Header）と送信元ポート番号で解析したグラフ

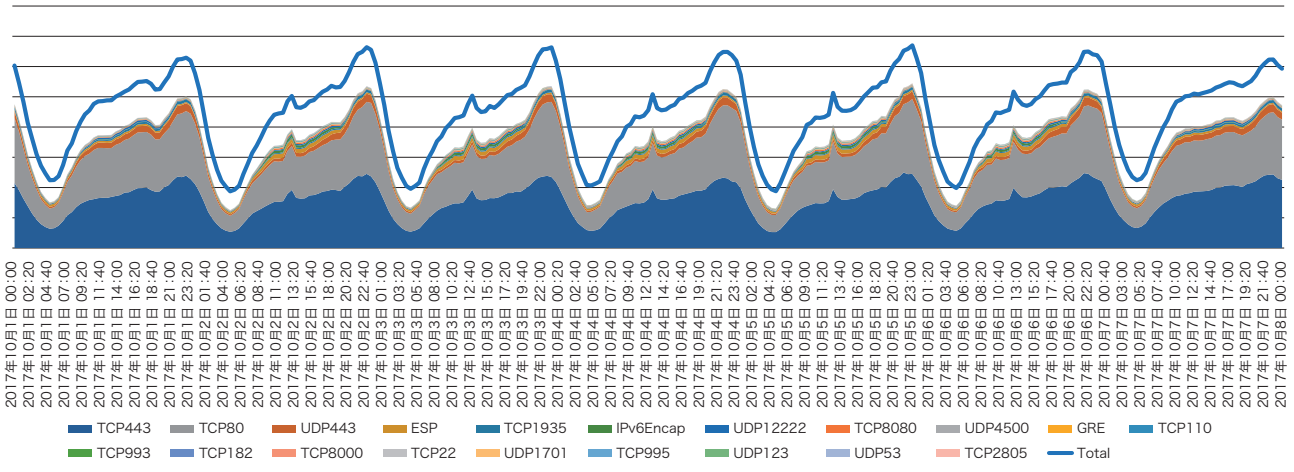

図-10 IPv4トラフィックのProtocol番号と送信元ポート番号で解析したグラフ

Theme 04

モバイル

モバイルのトラフィック傾向について、今回は1日の時間帯を軸に分析してみます。

図-11はある平日営業日の1日のトラフィック(bps)の推移です。縦軸は相対的なトラフィック量をあらわしており、グラフは変動の推移を示しています。昨今、モバイルサービスの利用者の大部分はスマートフォンを利用しています。スマートフォンが使われるシチュエーションを考えると想像できるとおり、グラフには大きな山が3つあり、それぞれ朝の通勤・通学時間帯、昼休み、夕方の退勤・下校後の時間にピークを迎えています。また、23時半以降にトラフィックが極端に下がります。

特に12時前後に利用が最も集中していることが分かります。朝夕の通勤・通学は時間的に分散しますが、昼休みは12時からという時間に集中しているのが原因でしょう。この時間帯には輻輳が発生しています。TCP/IPの仕組み上、輻輳が発生した場合はトラフィックが抑制されますが、にもかかわらずこれだけトラフィックが出ています。事業者にとっては、スマートフォン以外の需要を開拓することにより、時間帯によるトラフィックの平準化を図り、設備の稼働率を上げることが重要ですが、簡単ではありません。

図-12のグラフはある1週間のトラフィックグラフです。月曜日から金曜日まで、同じようなパターンの繰り返しが見られます。土曜日と日曜日はお昼12時のピークが小さく、その代り日中のトラフィックの落ち込みがありません。そして、日曜日から月曜日にかけての夜の谷が深くなっています。このグラフでは分かりにくいのですが、夜のトラフィックの谷は週末にかけて浅くなって行く傾向があります。我々の日々の営みを反映した興味深い事象です。

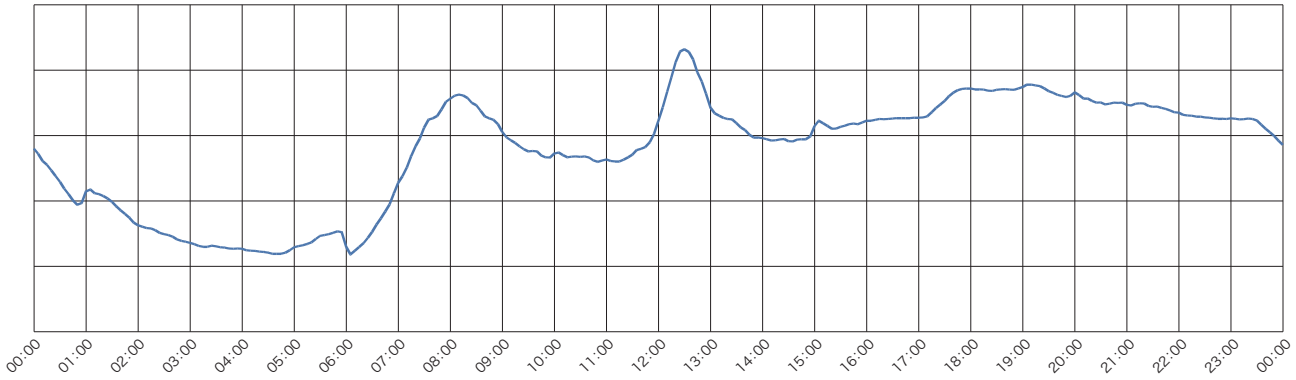

図-11 1日のダウンロードトラフィック推移

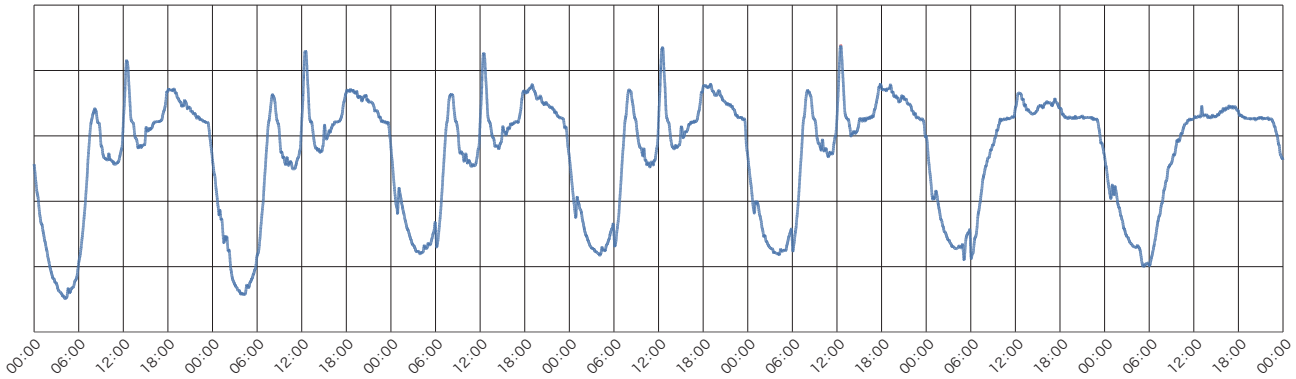

図-12 1週間のダウンロードトラフィック推移

図-13は、トラフィックグラフから計算した1日のデータ転送量を日付ごとにプロットしたものです。これは10月のグラフですが、年末年始をはじめとする大型連休のある月以外はほぼ同じ傾向です。週頭は転送量が少なく、金曜日に向けて転送量が増えていき、土日になると転送量が下がります。週末に向けて転送量が上がって行くのは夜間の転送量が週末にかけて増えて行くためでしょうか。また、土日の転送量が下がるのは家でブロードバンドなどへオフロードが行われているためだと考えられます。興味深いのは月末に向けて転送量が下がって行くことです。毎月割り当てられる通信量を使い切ってしまったユーザの通信が減るためと考えていますが、裏付けは取れていません。月が変わると、月末にかけて減っていた転送量は回復し、元の水準かそれ以上に戻ります。1年を通じて見ると、モバイル全体のトラフィックは着実に増えています。

スマートフォンは一部の人にとっては生活に密着し、必要不可欠なものになっています。モバイルのトラフィック傾向も、それを如実に表しています。

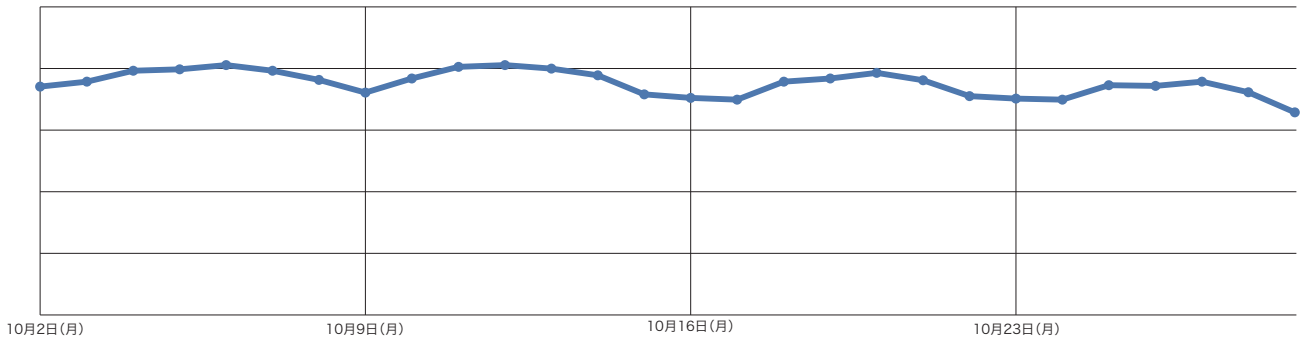

図-13 日付ごとデータ転送量

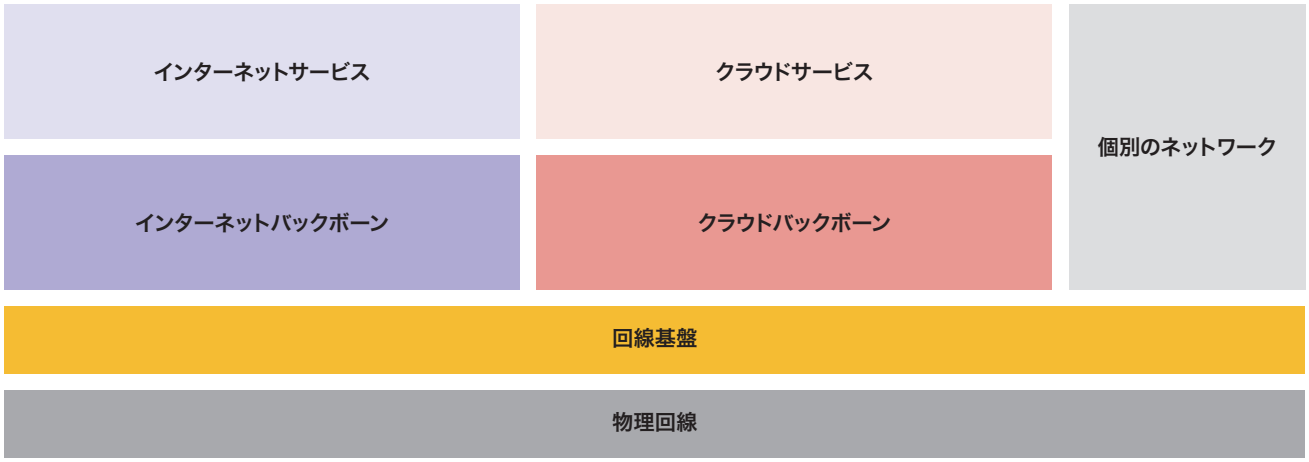

図-14 IIJ BackBone Structure

Theme 05

IIJインフラ(バックボーン)

ここではIIJのバックボーンインフラについて紹介します。

トラフィックは順調に増加しています。インターネットトラフィックについては全体で年平均1.35倍、日米回線は年平均1.2倍のペースで増加(いずれも過去4年間)しています。IIJ GIOサービスをはじめとするクラウドトラフィックについても2年半でおおよそ2.5倍に伸びています。

このようなトラフィック増加に対応するためにバックボーンインフラも変化してきました。規模の点では、3年前に東名阪に導入した100G回線は地方POP、日米、更には米東海岸まで延伸しています。一方、構造の点でも変化しています。現在のバックボーンインフラは物理回線の上に仮想回線を提供するためのレイヤー2の閉域網(回線基盤)を構築し、インターネット及びクラウド用のバックボーンはその回線基盤が提供する仮想回線上で構成されています。インターネットトラフィックならびにクラウドトラフィックを同一物理回線で提供し、レイヤー2閉域網でトラフィックエンジニアリングを実施することで回線の利用効率を向上させ、コストメリットを大きくしています。またこの構造変化により地理的な制限に縛られず自由にネットワークを構築できるようになったことも大きなメリットとなっています。昨年度リリースしたIIJ DDoSプロテクションサービスの大規模攻撃対応の新品目も、この構造変化があったからこそリリースできたと言えます。今後もインターネット、クラウド問わず様々なネットワークサービスを提供するためにバックボーンインフラを変化させ続けていきます。

執筆者:

1.BGP・経路数
倉橋 智彦(くらはし ともひこ)
IIJ サービス基盤本部 インフラ企画部

2.DNS
松崎 吉伸(まつざき よしのぶ)
IIJ サービス基盤本部 インフラ企画部

3.IPv6
佐々木 泰介(ささき たいすけ)
IIJ サービス基盤本部 インフラ企画部

4.モバイル
篠井 隆典(ささい たかのり)
IIJ サービス基盤本部 ネットワーク技術部 モバイル技術課

5.IIJインフラ(バックボーン)
菅原 大輔(すがわら だいすけ)
IIJ サービス基盤本部 ネットワーク技術部 バックボーン技術課

VSSはユーザデータを守らない

2.1 はじめに

VSSはVolume Shadow Copy Serviceの略で、Windows XP/Windows Server 2003以降に搭載されているバックアップ関連の機能です。

VSSはスナップショットを作成することができ、ある時点のボリュームの状態を保存することができます。ユーザはスナップショットを参照することで、スナップショットを作成した時点のボリュームのデータにアクセスすることができます。これには削除したファイルやデータが変更されたファイルも含まれます。また、スナップショット上のデータはリードオンリーであるため更新されません。更にボリューム上でファイルがロックされていても、スナップショット上のファイルはロックされません。これらの特性を利用するとデータの完全なバックアップを行うことができます。

Windows 7/10のファイルやフォルダのプロパティに表示される「以前のバージョン」タブから復元できるファイルもスナップショットを利用しています(図-1)。ランサムウェアが流行した際にスナップショットからファイルを復元する方法が紹介されていたことを記憶している人も少なくないでしょう。

スナップショットは攻撃者が使用した攻撃ツールや一時ファイル、改ざんされたファイルなどの復元に利用できるため、デジタルフォレンジックにおいても非常に重要なデータの1つとして、解析者たちに認識されています。しかし今回、デジタルフォレンジックの技術調査を行う中で、VSSを有効にしていてもユーザのデータがスナップショットに正常に保存されない事象をWindows 8.1/10で確認したため、その原因と影響範囲を調査しました。また、事象の対処方法についても紹介します。

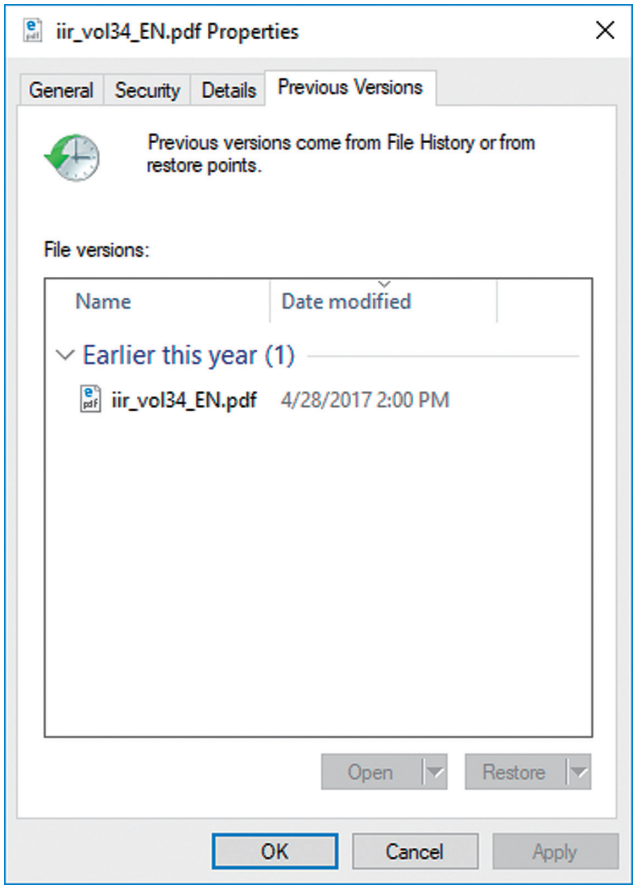

図-1「以前のバージョン」タブ

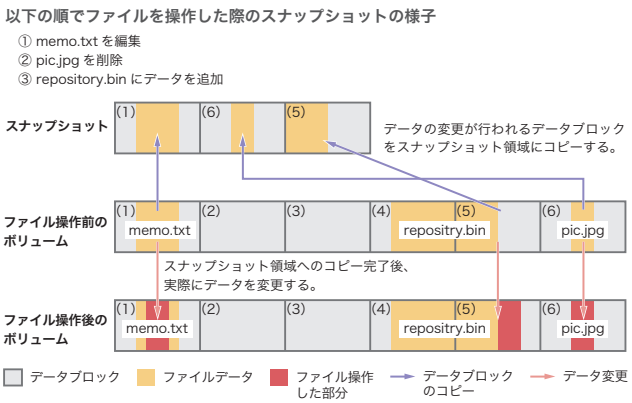

図-2 差分データ保存の仕組み

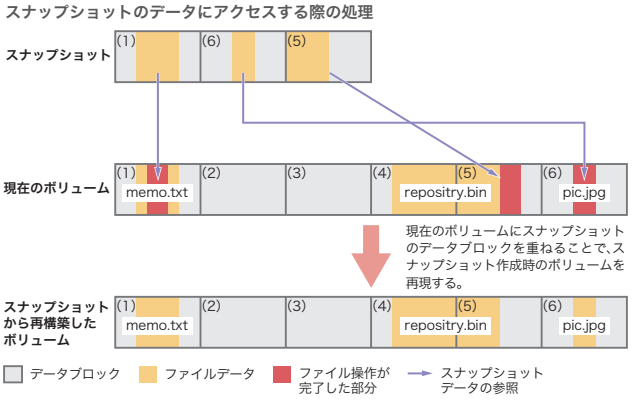

図-3 スナップショットアクセスの仕組み

2.2 VSSスナップショットの仕組み

前述したように、スナップショットはある時点のボリュームの状態を保存しますが、ファイル単位でデータの保存を行っているわけではありません。例えば、1GBのファイルの内、1MBを変更した際にファイル全体を保存するのは、ボリュームの使用効率が悪い上にOS全体のパフォーマンスも低下してしまいます。

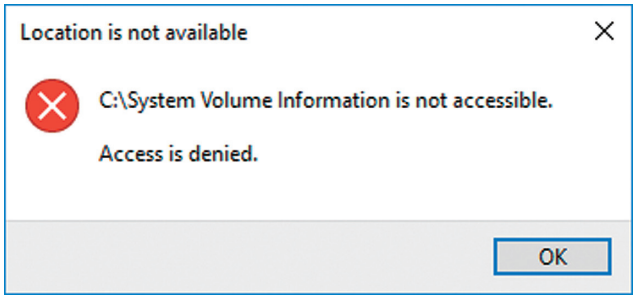

図-4 スナップショットはユーザアクセスから保護されている

そのため、スナップショットには差分データのみが保存されます。ボリューム全体を16KBごとのデータブロックに分割し、スナップショット作成後に変更が発生したデータブロックのデータをそのオフセットと共に保存したものが差分データとなります(図-2)。スナップショット上のファイルにアクセスする際には、現在のボリュームデータにスナップショットの差分データを透過的に統合して、スナップショット作成時のデータを再構築します(図-3)。

2.3 VSSスナップショットのファイル構成

スナップショット関連のファイルはボリュームのルートフォルダ直下の「System Volume Information」フォルダに保存されていますが、通常はエクスプローラなどではアクセスすることができません(図-4)。図-5ではFTK Imager[*1]を使用してファイルを表示しています。

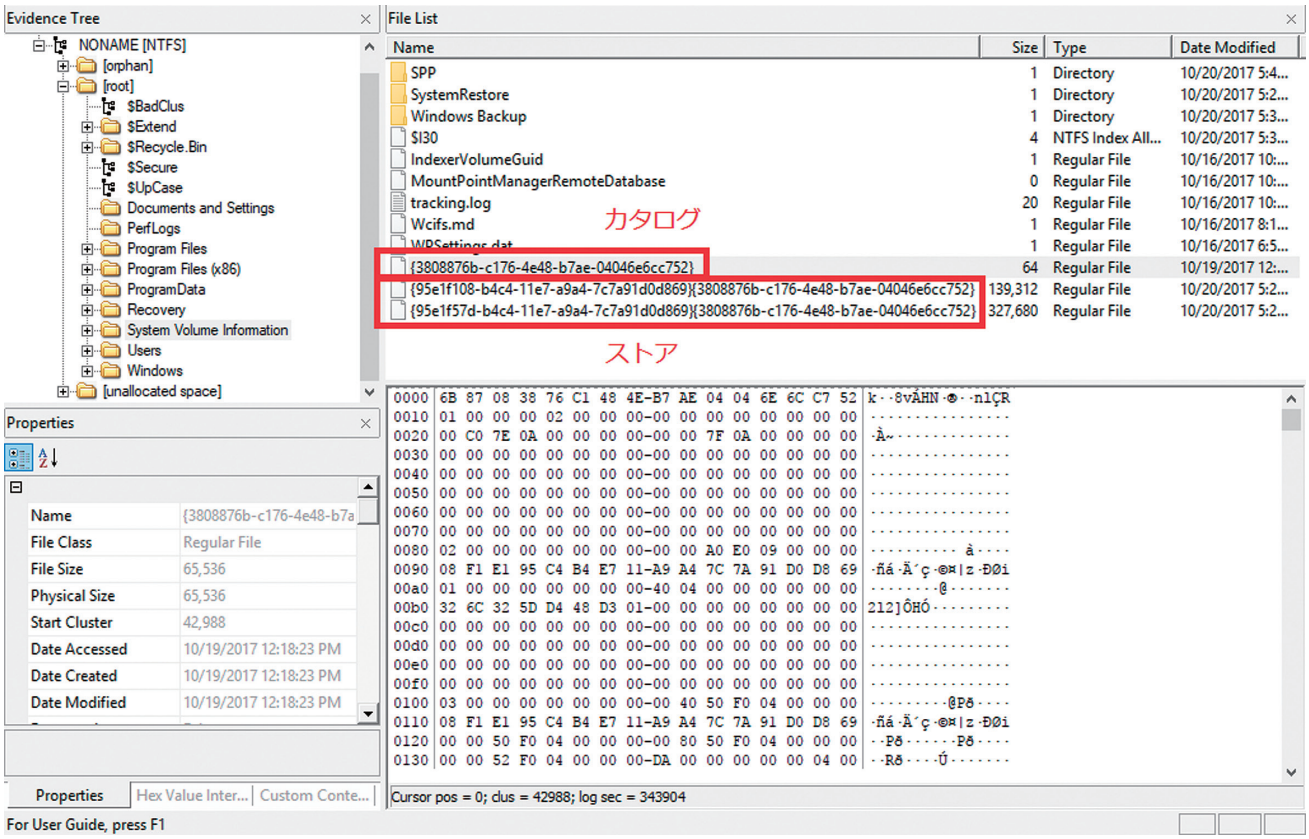

図-5「System Volume Information」フォルダ内のファイル構成

*1 FTK Imager(https://accessdata.com/product-download)。

スナップショットは「カタログ」と「ストア」という2種類のファイルから構成されています。カタログは「{*カタログGUID*}」というファイル名で、スナップショットの生成日時やストアのGUIDといったメタ情報を記録しています。ストアは「{*ストアGUID*}{*カタログGUID*}」というファイル名でスナップショットのデータ本体になります[*2]。

2.4 VSS有効化とスナップショットの操作

VSSは「システムのプロパティ」で有効か否か確認することができます(図-6)。無効になっている場合は「構成(Configure)」ボタンをクリックして、「システム保護対象」ダイアログを表示します。そして、「システムの保護を有効にする(Turn on system protection)」を選択し、「ディスク領域の使用量(Disk Space Usage)」を設定後、「OK」ボタンをクリックします(図-7)。スナップショットを手動で作成する場合、図-6の「作成(Create)」ボタンをクリックします。

なお、同一のボリューム内にスナップショットを複数作成することができますが、図-7で設定した「ディスク領域の使用量」を超える場合、もっとも古いスナップショットが削除されます。

作成したスナップショットのリストの確認や削除などは、vssadmin.exeで行うことができます。管理者権限のコマンドプロンプトから、「vssadmin.exe list shadows」を実行するとスナップショットのリストを取得することができます(図-8)。その他、WMIやPowerShellからスナップショットを操作することも可能です。

2.5 ファイル復元テスト

ユーザが作成したファイルがスナップショットに正常に保存されるか検証するために、スナップショットに保存されたファイルを復元するテストを行います。ユーザデータとして、弊社のWebページで公開しているIIR Vol.26からVol.35の10個の

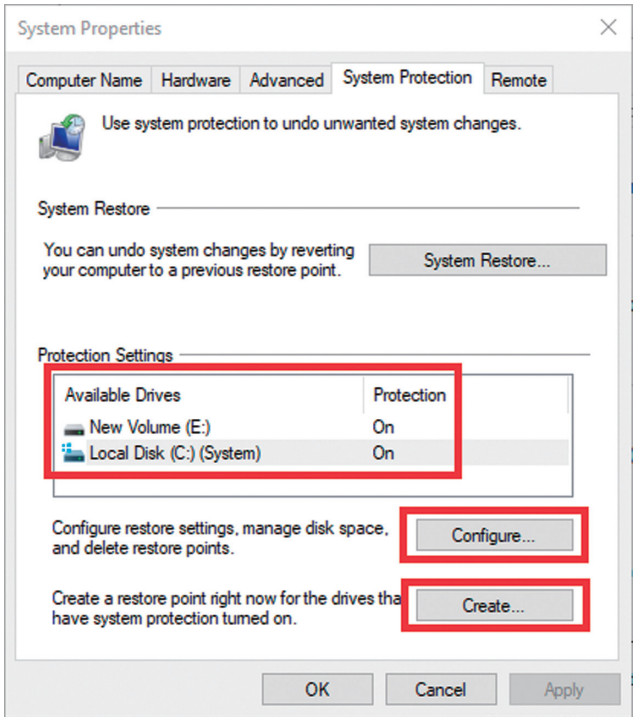

図-6「システムのプロパティ」ダイアログ

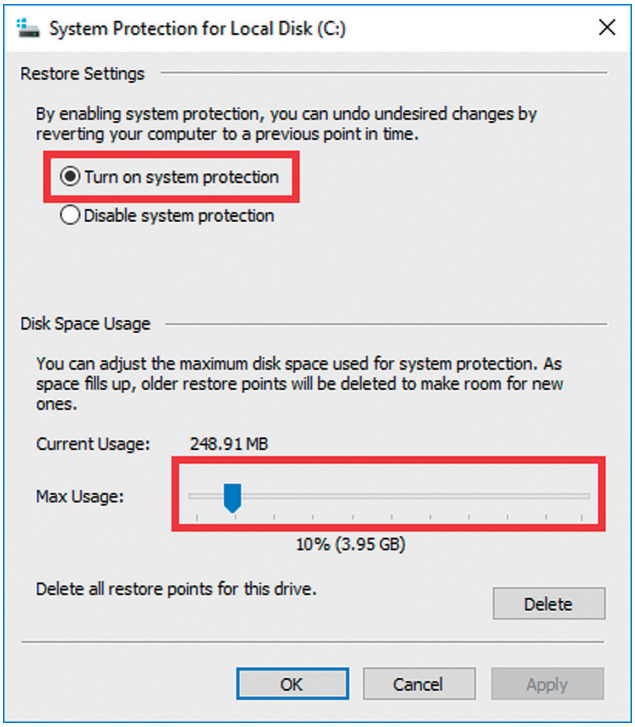

図-7「システム保護対象」ダイアログ

*2　今回はスナップショットのファイル構成やデータ構造については取り扱わない。詳細について知りたい場合、Volume Shadow Snapshot(VSS)(https://github.com/libyal/libvshadow/blob/master/documentation/Volume%20Shadow%20Snapshot%20(VSS)%20format.asciidoc)が非常に参考になる。

PDFファイルをデスクトップの「PDF」フォルダに保存し、スナップショットを作成しました。

ファイル削除ツールであるSDelete[*3]を使ってPDFフォルダ内のファイルを削除し、その後、ShadowExplorer[*4]を使用してスナップショットからデータを復元します。

Windows 7 SP1とWindows 10 1703の環境でこの作業を行い、それぞれのスナップショットから復元したPDFのMD5ハッシュ値[*5]を表-1にまとめました。Windows 7ではすべてのファイルが正常に復元できたのに対して、Windows 10ではすべてのファイルが破損していました。

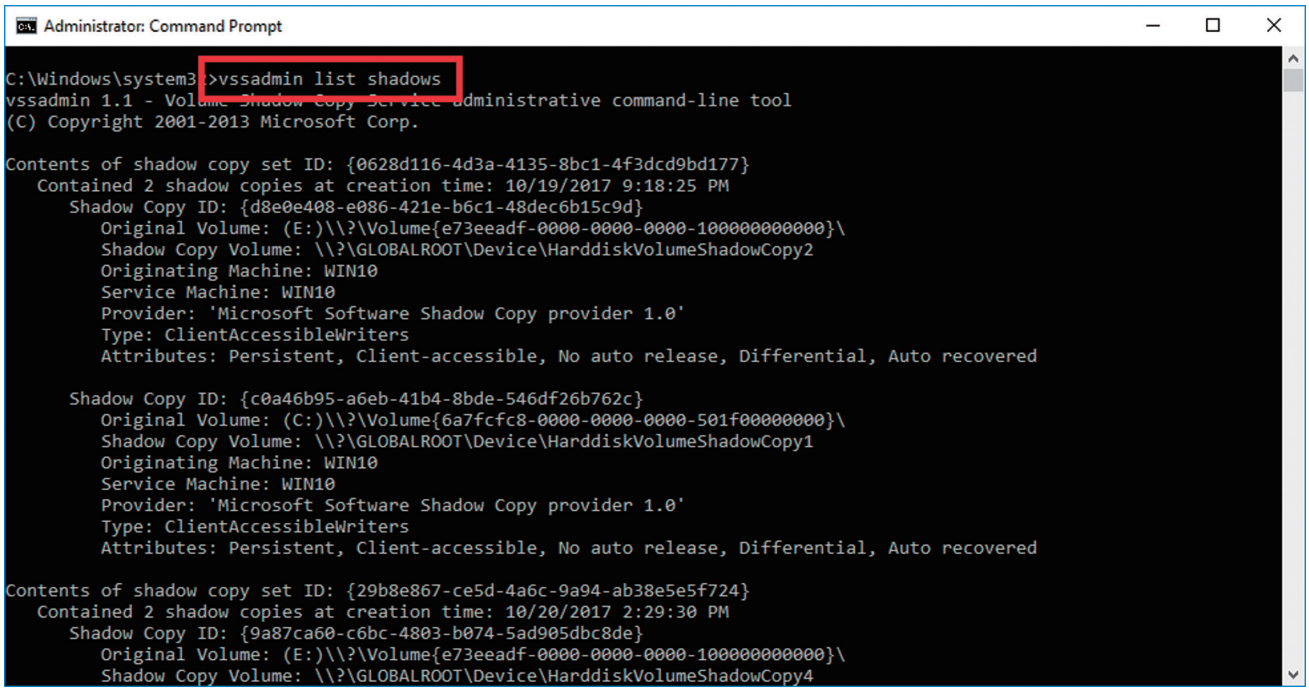

図-8 スナップショット一覧

ファイル名	元ファイルのMD5	Windows 7 SP1		Windows 10 1703	
		復元したファイルのMD5	一致	復元したファイルのMD5	一致
iir_vol26_EN.pdf	a3002c631ca894034b594ec4e1a7c285	a3002c631ca894034b594ec4e1a7c285	○	42b4ac3f7e2f349ed8a0d3e240db35a6	×
iir_vol27_EN.pdf	09339fc3375988f8f769ccfa7ac75d4f	09339fc3375988f8f769ccfa7ac75d4f	○	e4986e8866435b7273f16a7f8fe60a14	×
iir_vol28_EN.pdf	89fee5ffccfb5be9749639e7e65a218e	89fee5ffccfb5be9749639e7e65a218e	○	86ff8c095a5b116e1ff34e12d6999053	×
iir_vol29_EN.pdf	42edeccedd51eecc20d0d9c123329b9a	42edeccedd51eecc20d0d9c123329b9a	○	5a8a530c084e5ee8ec129c62afa5ab0e	×
iir_vol30_EN.pdf	25df11281a2b1fb72a3f6d48d697c6b4	25df11281a2b1fb72a3f6d48d697c6b4	○	a4a68b122007b80a24ca2457e69b0902	×
iir_vol31_EN.pdf	79eac7926477141397f179654d307473	79eac7926477141397f179654d307473	○	b8cac677d7cf6bf15594a477c4b1b104	×
iir_vol32_EN.pdf	a99869ea8ea3cbda032d36ba000cdd26	a99869ea8ea3cbda032d36ba000cdd26	○	1bd79719c9c91c52e1de214a16572f90	×
iir_vol33_EN.pdf	a246c3f7ef836a141eb9c181899003f3	a246c3f7ef836a141eb9c181899003f3	○	17b820ab7f61a6de25cfcc89a1f49e62	×
iir_vol34_EN.pdf	093f3757b7a9269655d9fa6816b6dc72	093f3757b7a9269655d9fa6816b6dc72	○	b3c354a635ec62d747ae20aa71f46ab0	×
iir_vol35_EN.pdf	256dd74e71e1080170ddf59d0757e230	256dd74e71e1080170ddf59d0757e230	○	6220ce0b3df16961123438bd524568ce	×

表-1 復元ファイルの比較

*3 SDelete(https://technet.microsoft.com/ja-jp/sysinternals/sdelete.aspx)。
*4 ShadowExplorer.com(http://www.shadowexplorer.com/)。
*5 MD5ハッシュが衝突しやすいことは知られているが、特定ファイルの同一性の比較であること、また、紙面の広さの制限から採用した。

2.6 ファイル破損の原因と対策

破損しているファイルを正常なファイルとバイナリエディタで見比べると、ファイルの一部がNullバイト(0x00)で置き換わってしまっていることが分かります(図-9)。左がオリジナルのファイルで右がWindows 10から復元したファイルです。赤い箇所がデータの異なっている部分になります。ファイルによって、Nullバイトに置き換わっている箇所は異なります。

調査の結果、スナップショットのユーザデータが破損する原因はWindows 8から導入された「ScopeSnapshots[*6]」という機能であることが分かりました[*7]。この機能が有効になっている場合、スナップショットに保存する対象のデータがWindowsのシステムに関連するファイルのみに限定されるため、ユーザデータはスナップショットに保存されなくなります[*8]。この機能はシステムボリューム(Cドライブ)のみに適用されますが、近年のPCのドライブ構成はCドライブのみということも珍しくないため、この機能の影響は大きいと言えます。

機能仕様の詳細が公開されていないので、テスト結果からの推測を含みますが、ファイルを限定する動作は完璧に制御されているわけではないようで、ユーザデータの一部だけがスナップショットに保存される場合もあります。このような不完全なユーザデータを復元しようとした際に不足しているデータ部分が0x00に置き換わっている可能性があります。なお、ファイルがレジデント[*9]であればユーザデータであっても、スナップショットに保存されていました。

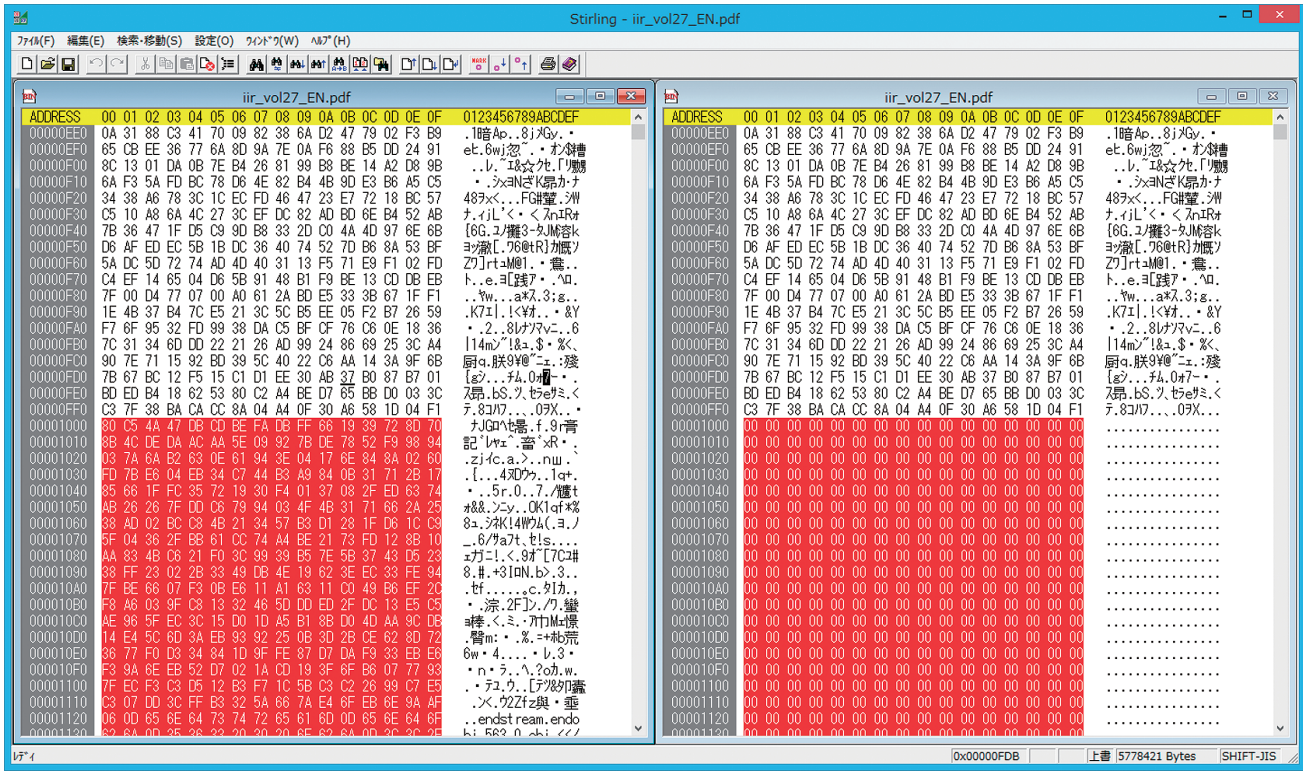

図-9 正常なデータと破損データの比較

*6 Calling SRSetRestorePoint(https://msdn.microsoft.com/ja-jp/library/windows/desktop/aa378727(v=vs.85).aspx)。
*7 マイクロソフトからも、この機能が原因である可能性が高い旨の回答を得ている。
*8 このような仕様変更が行われた理由は公にはなっていないが、すべてのデータをスナップショットに保存することのパフォーマンスの問題やスナップショット用領域の使用効率の問題、ユーザデータの肥大化、ユーザデータのバックアップに「ファイル履歴」が推奨されるようになったことなどが関係していると推測される。
*9 NTFSはファイルデータが小さい場合、データ用に領域を確保せず、NTFSのMFTレコード内の$DATAアトリビュートに直接保存する。この状態をレジデントと呼ぶ。

ScopeSnapshotsはレジストリの「HKLM\Software\Microsoft\Windows NT\CurrentVersion\SystemRestore」キーに「ScopeSnapshots」という名前でDWORD値「0」を設定し、OSを再起動することで無効化できます(図-10)。ScopeSnapshotsを無効化したWindows 10で、スナップショットからユーザデータが正常に復元できることも確認しています[*10]。

確認した限り、サーバ系Windowsでは、ScopeSnapshotsの無効化なしでスナップショットからユーザデータを正常に復元することができました。デフォルト設定のOSごとに復元したユーザデータの破損の有無を表-2にまとめました。

2.7 まとめ

VSSはWindows XPの頃から存在する機能ですが、OSのバージョンアップに伴って仕様が変更されていたことが今回分かりました。このように従来から使用されていた機能でも仕様が変更される場合があるため、OSのリリースなどに合わせて、仕様変更の確認や使用しているツールの検証を行うことが重要です。

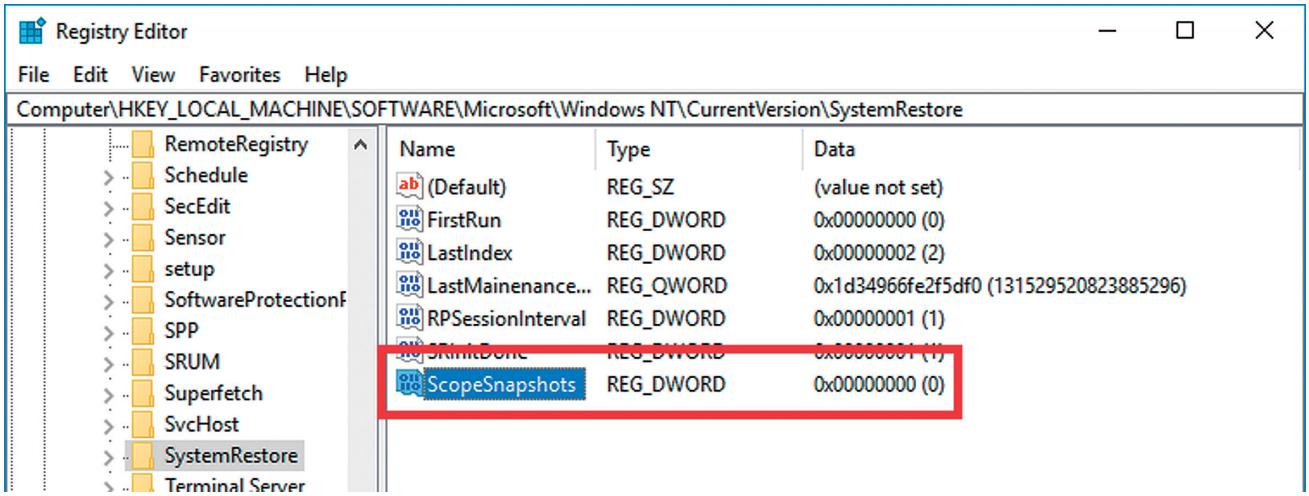

図-10 ScopeSnapshots無効化の設定

表-2 OS別復元したユーザデータの破損の有無

	Windows 7 SP1	Windows 8.1	Windows 10	Windows Server 2012/2012 R2	Windows Server 2016
復元したユーザデータの破損	なし	あり	あり	なし	なし

執筆者:
齋藤 衛(さいとう まもる)
IIJ セキュリティ本部 本部長、セキュリティ情報統括室 室長兼務。法人向けセキュリティサービス開発などに従事の後、2001年よりIIJグループの緊急対応チームIIJSECTの代表として活動し、CSIRTの国際団体であるFIRSTに加盟。ICT-ISAC Japan、日本セキュリティオペレーション事業者協議会など、複数の団体の運営委員を務める。

小林 稔(VSSはユーザデータを守らない)
IIJ セキュリティ本部 セキュリティ情報統括室

*10 Windows 8.1でも一連の検証を行ったが、Windows 10と同様の結果になった。

商用化を迎えたVideo over IP技術とその経済圏

Video over IPは技術面でもビジネス面でも、まさにいま夜明けを迎えています。標準規格の発刊が2018年に見込まれており、各メーカは競い合うように規格準拠を謳っています。放送局でも急速に関心が高まっており、北米や欧州はもとより、日本での放送機器展でも特集セッションが組まれるようになりました。本稿では多くの関係者が期待する技術であるVideo over IPについて説明します。

3.1 あらゆるものがIPに

インターネットが普及期に突入してから既に20年とも30年とも言われます。この間、様々なメディアがIPをインフラとして用いるようになりました。印刷技術を用いてきた新聞や雑誌、書籍などのメディアはかなり早い段階からWorld Wide Webに取り組んでいます。電話という技術が従来の回線交換型ネットワークからIPへその基盤を移したことも、エポックメーキングな出来事として記憶されるでしょう。これまでの「電信電話会社」が「通信事業者」に姿を変えた(変えざるを得なかった)瞬間だったからです。ラジオはストリーミング技術を応用することで、IP上でのメディアとしての存在を確立しつつあります。テレビジョン放送も、積極的にIPテクノロジーを獲得しようとしています。テレビリモコンの「dボタン」でお馴染みのデータ放送は、2013年にハイブリッドキャストへと進化した時点でストリーミング技術を採用しました。また4K/8K放送は放送波そのものがIPのフォーマットになっています。このように多くのメディアがIP技術を獲得、活用しはじめています。

この流れの中で最大、かつ最後のものが「映像・音声信号」です。それもストリーミング技術では扱われてこなかった、圧縮されていない音声・映像信号そのもの(「ベースバンド」とも呼ばれます)が、IPの上に乗ろうとしているのです。

規格名	映像信号(画角とフレームレート)	ビットレート
HD-SDI	1080i30	1.485Gbps
3G-SDI	1080p60	2.97Gbps
6G-SDI	2160p30	6Gbps
12G-SDI	2160p60	12Gbps

表-1 SDIの種類と帯域

3.2 ベースバンドと同軸ケーブル

このベースバンドはどのようなところで取り扱われているか。メインとなるユーザは放送局やスタジオです。このような環境では信号品質を可能な限り確保することが好まれます。例えば放送局の場合、放送波となって電波になる前の段階で、映像信号は圧縮されてしまいます。この最終段までは、映像信号の品質は高く保たれる必要があります。圧縮プロセスにノイズ成分が多い映像を投入すると、どうしても映像品質は劣化するからです。逆にいえば、視聴者がテレビジョンで視聴している映像は、元々は相当品質の高いものなのです。こうした環境では映像信号の物理伝送メディアとして同軸ケーブルが使われてきました。同軸ケーブルを断面で見ると、内部導体を絶縁体が包み、その外に外部導体、一番外側に保護被覆が覆う形になっています。これまで高周波を伝送するためによく用いられてきており、またノイズに強い耐性を持っています。しかし同軸ケーブルはその特性上、より多くの電気信号を伝送したい時、長距離に伝送しようとする時には、電気信号の減衰に備えてケーブルの径を大きくする必要があります。

同軸ケーブルを使った映像伝送規格としては「SD-SDI(270Mb/s, 1990年)」「HD-SDI(1.5Gb/s, 1998年)」「3G-SDI(3Gb/s, 2002年)」「6G-SDI(6Gb/s, 2015年)」が規定されてきました。これらはSMPTEで策定されたもので、Serial Digital Interfaceという名前が付いています。4K放送で実施されるのは毎秒60フレームですので、毎秒30フレームまでの6G-SDIでは対応できません。そこで「12G-SDI」という4K対応の伝送フォーマットが2017年に規定されています。4Kの現場では12G-SDIが使われることになるでしょう。

実は現状では3G-SDIを4本束ねて4Kの映像を伝送する手法も使われています。しかし同軸ケーブルが4本ともなると、取り回しが

大変になってしまいます。あくまで過渡的な手段として用いられているもので、いずれ12G-SDIへの移行が求められるでしょう。

しかし12G-SDIは、大容量データを伝送するために距離を伸ばすことができず、取り回しが不十分になるという問題があります。概ね数十メートルといった距離しか届きません。そこでメーカ各社は12G-SDIの開発に着手すると同時に、次世代の物理伝送メディアとして光ファイバに着目しました。今後4Kや8Kの普及を考えると、いずれ同軸ケーブルでは十分な帯域が賄えなくなることは明らかです。既に通信業界では光ファイバの利用は一般的になっていますので、これは自然な選択だったといえます。そしてその際、光ファイバの上位プロトコルとしてEthernetそしてIPが選択されたというわけです。EthernetもIPも十二分に普及している技術であり、かつ今後の発展の余地があります。独自のプロトコルを生み出すよりも、既存の「今ここにある技術」を採用する。その方がより簡単かつより早い時期に、光ファイバによって手に入る大容量伝送を具現化できると踏んだわけです。

3.3 SMPTEでの標準化

2017年、Video over IP関連のキーワードになったのは「SMPTE ST 2110」という規格です。最終的な発刊は2018年と見込まれていますが、本命となる規格と捉えられています。まだ発刊されていないにもかかわらず、リリース時の対応を謳うメーカが急速に増えています。それほどまでに業界内での期待値が高い規格といえるでしょう。

SMPTEとはThe Society of Motion Picture and Television Engineersの略語です。米国映画テレビ技術者協会と訳されますが、発刊する規格は米国のみならず世界中に大きな影響を与えます。つまり、グローバルスタンダードを担う標準化団体の役割があります。

SMPTE ST 2110は"Professional Media Over Managed IP Networks"と銘打たれた規格です。プロフェッショナルメディアとは放送局などで用いられる技術であることを意味しています。また管理されたIPネットワークとは、インターネットではなくクローズドな網を想定していると考えられます。このST 2110は複数の規格より構成されており、"protocol suite"とも呼ばれています。つまりST 2110はVideo over IP規格として集大成となることが予測されます。

ST 2110に先行する技術として、メーカによる独自のVideo over IP実装がありました。メディアグローバルリンクスのIP-VRS(IP Video Routing System, 2008-)、Evertz MicrosystemsのAspen(2013-)、SonyのNMI(Networked Media Interface, 2014-)がそれで、どちらも既に市場にリリースされ実用に供されています。これらの各社は他社に先駆けて技術開発を進めたが故に、独自の規格を策定せざるを得なかった事情があります。これらは現在でもST 2110に先行する機能を持っています。しかしEvertzはSMPTE ST 2110への対応をアピールし始めましたし、Sonyも2110対応ゲートウェイやCCUをデモ展示・発表しています。先行するメーカは自らの技術とST 2110

規格番号	規格名	概要と特徴
2110-10	System Overview	System timing model & Session Description
2110-20	Uncompressed Video	Based on RFC 4175 32k x 32k, 4:2:2, 4:4:4, HDR(PQ, HLG)etc.
2110-30	PCM Audio	Based on AES67
2110-21	Traffic Shaping	
2110-22	Compressed Video	TBC
2110-31	AES3 Transparent Transport	Includes compressed audio
2110-40	Ancillary Data	Captions, subtitles, time codes, active format description, dynamic range, etc.

表-2 SMPTE ST 2110の公表されている規格一覧

との融和によって生まれるメリットの追求が課題でしょうし、後発のメーカは標準化の大きな流れにあって自らの特色をいかに磨くかがテーマになっていくでしょう。

2110の開発にあたっては、こうした先行技術の存在にも助けられたに違いありません。既にプロダクトレベルで動いている技術があったからこそ、標準化への確信と意欲が湧き上がったのではないかと想像します（先行技術を持つ側からすれば、今さら…という気持ちもあることでしょうし、逆に自らの行動の正しさが確証されたという思いがあるかも知れません）。

SMPTEはこのST 2110の規格化にあたり、既存の規格を有効に利用するアプローチを採っています。具体的にはIETF（The Internet Engineering Task Force）のRFCに対する参照です。RFCで策定された規格の中に、マルチメディア通信のために開発されたプロトコルがあります。RTP（Real-time Transport Protocol）です。RTPはVoIP（Voice over IP）などでの多数の実績があり、様々なデータペイロードを扱うことができる拡張性があります（実際にはデータフォーマットごとに規定策定し、RFCを発刊していくことになります）。またマルチキャストとも親和性があり、事実多くのマルチキャストアプリケーションで使われてきました。こうした背景を持つRTPは、Video over IPにとってもうってつけのプロトコルだったわけです。

オーディオはVideo over IPよりもIP化では先行していました。Ethernetのフレームにそのままオーディオデータを載せた規格はCobraNETがあり、これらがAudio over IPの原型といえるでしょう。そしてIPを利用するようになったDante

	Sony IP Live	Evertz Aspen	VSF TR-03 (SMPTE 2110)	VSF TR-04	SMPTE 2022-5/6	IntoPix TICO
Uncompressed Video	NMI	RDD 37 Video PES	RFC 4175	SMPTE 2022-6	Yes	SMPTE 2022-6
Uncompressed Audio	NMI	SMPTE ST 302 Audio PES	AES67 / RFC 3190	AES67 / RFC 3190	Embedded	SMPTE 2022-6
Compressed Video	LLVC	No	No	No	Opt JPEG2K	Yes
Metadata	NMI	SMPTE ST 2038 Meta PES	IETF RTP Proposal	SMPTE 2022-6	Embedded	SMPTE 2022-6
Forward Error Correction	Frame Aligned	No	No	No	Not Aligned	No
Independent Packetization	NMI	TS over SMPTE 2022-2	Yes	No	No	No
Registration and Discovery	Plug & Play (NDCP)	JSON-RPC	AMWA IS-04	AMWA IS-04	No	No
Connection Management	Sony IP Live System Manager	Evertz MAGNUM	AMWA IS-05	AMWA IS-05	No	No
Timing / Sync	SMPTE 2059	TS PCR/PTS	RFC 4566 (SDP)	RFC 4566 (SDP)	No	No
COTS IP Switch	Yes	No	Yes	Yes	Yes	Yes
SMPTE Standard	RDD 34 (LLVC) RDD 40 (NMI) RDD 38 (NDCP) SMPTE 2059 (PTP)	RDD 37 (ASPEN)	VSF Reccomendation (SMPTE 2110 in Process)	VSF Reccomendation	SMPTE 2022-5/6	RDD 35 (TICO)
Interoperability	Guaranteed	Demonstrated	Demonstrated	Demonstrated	Demonstrated	Within TICO Family
Endpoint Validation	Sony Testing Lab	No	No	No	No	No

表-3 Nextera Video社によるVideo over IP Comparison*1

*1　Nextera Video、"Video over IP Comparison"（http://www.nexteravideo.com/resources）。

(Digital Audio Network Through Ethernet)。このプロトコルはAudinateによって2006年に発表されると人気を博し、日本でもYAMAHAなどが採用しています。しかしこの技術はプロプライエタリなもので、ライセンスが必要でした。続いて2011年、Ravennaが登場します。RavennaはDanteに比べるとより標準的な技術が使われているのが特長です(ラベンナはフィレンツェ出身の詩人ダンテが客死した街の名前です)。そしてAudio Engineering Societyによって2013年にはAES67(AES standard for audio applications of networks - High-performance streaming audio-over-IP interoperability)が登場し、Audio over IPの標準化がなされました。しかし現状でもDanteやRavennaはかなり混在して使われている状況です。

マルチキャストは1986年、RFC988として発刊された技術です。IPはパケットのヘッダにIP source address情報とIP destination address情報を持ちます。IP addressは一意に1つずつノードに割り振られますので、通信は1対1で行われることを想定しています。この通信の方式をユニキャストと呼びます。しかしマルチキャストはIP destination addressに「host group」という概念をあてはめることで、送信者と受信者を1対他の関係にすることを実現しています。このhost groupというのは、例えて言えばテレビのチャンネル、ラジオの周波数のようなものです。そのグループに属すという手続きを踏んだ全員が、同じデータを同時に受信できると思えば良いでしょう。このためにhost group用に特別なIPアドレスが割り当てられています。

マルチキャストは一時期インターネットでも期待された技術で、世界規模での実験も多く行われていました。放送型アプリケーションには最適なものと考えられたからです。1994年にローリングストーンズがライブコンサートの模様をマルチキャスト中継したことは、今では伝説となっています。IIJも、IIJ4Uの接続サービスにおいてマルチキャスト受信オプションを提供したことがありました。

Video		Audio	Ancillary
2110-20	2110-22	2110-30	2110-40
非圧縮ビデオ	圧縮ビデオ	PCM音声	SMPTE ST 291
RFC4175	今後策定	AES67	RFC発刊待ち
RTP RFC3550			
UDP RFC768			
IPv4 RFC791 (IPv6 RFC8200)			
Ethernet			
物理層			

図-1 SMPTE ST 2110とRFCの関係を階層構造で示したもの

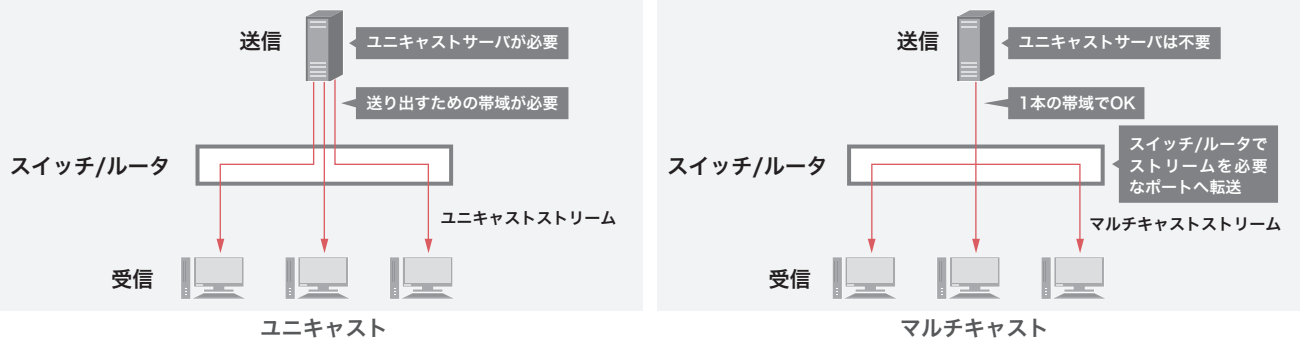

図-2 ユニキャストとマルチキャストの比較

その後マルチキャスト技術はインターネットにおける相互接続の手法などがうまく解決できず、幅広く普及することはありませんでした。しかしクローズドなネットワーク環境を前提とすれば、現状でも有効性が高い技術といえます。放送制作の現場ではまさにこの「1対他」の伝送が行われているからです。1台のカメラで撮影された映像は要所要所で分岐していきます。SDIの世界でもルータと呼ばれる装置があり、SDIの入力を電気的に分配し、指定されたポートへ出力する役割を担っています。このフローはマルチキャストの挙動にそっくりなのです。

3.4 国際放送機器展での動向

放送業界において国際的なコンベンションといえばNABShowとIBCが有名です。NABShowは毎年4月にLas Vegasで開催され、10万人規模の参加者を集めます。一方IBCは毎年9月にAmsterdamで開かれ、来場者は5万人を越えます。それぞれ北米と欧州での放送業界事情を反映するため、ショーとしての雰囲気はやや異なります。メーカからすると約半年ごとに最大規模のコンベンションが巡ってくるため、それぞれのタイミングで新製品や機能リリースの発表が行われるなど、開発やマーケティングのマイルストーンとなっているようです。

そのNABShowとIBCでも、Video over IP技術は次世代の技術として脚光を浴びています。Video over IP機器の総合接続検証デモンストレーションである「IP Showcase」がIBC2016, NABShow 2017, IBC2017と引き続き開催されており、業界の注目を集めています。40を越えるVideo over IP機器メーカが相互接続検証のために集い、互いの機器の接続性を観客に対して展示したのです。

図-3 IBC2017でのIP SHOWCASEの模様

標準規格を採用するメリットの1つに相互接続性が挙げられます。様々の接続もできるようになるはずです。IPもSDIも元々そうした価値観と実績を持っていましたので、Video over IPでも相互接続性は当然のように期待されています。とはいえなかなかそう素直に接続が成功するものでもありません。規格書にはどうしても隙間があり、実装には個別の判断が存在し、メーカ機器間での挙動にギャップが生まれてしまうからです。

このIP Showcaseではコンベンション開催に先立ちホットステージが準備されており、技術者が「合宿」状態で缶詰になって検証する体制が組まれています。複数のメーカ同士で検証をする機会など普段ではあまりありませんので、こうした機会はメーカにとってもチャンスと捉えられているそうです。

3.5 なぜ、IPが採用されるのか

そもそも、IPのメリットとは何か。「双方向性」「多重化」「相互接続」という点が、SDIにはないIPの利点です。インターネットで発展してきたIPの観点ではどれも当たり前のことですが、放送機器にとっては新たな機能を獲得することになります。1本の光ファイバ(1芯もしくは2芯)を使えば、送信側と受信側の関係を固定する必要がなくなります。また、やはり1本の光ファイバを通じて複数の映像や、他のメディアを扱うことができるようになります。例えばオーディオやインカム、Webを使ったカメラの遠隔操作など、撮影にまつわる影像・音声・制御のすべてをIPで一本化することができるようになります。

更に、IPのメリットとしてネットワークとネットワークの接続が比較的簡単にできることが挙げられます。この相互接続に、ネットワーク間の物理的な距離は問題とされません。例えば光ファイバの減衰を補償するために伝送装置を区間ごとに設置するなど、遠距離接続に必要な問題解決は低レイヤーの技術に任すことができます。IPとしては距離を意識する仕組みになっていないため、遠隔地接続が簡単にできるようになるのです。もちろん遠距離になればなるほどIPパケットの伝送に必要とされる時間は伸びてしまいますが、これはIPに限った話ではありません。

また、SDI代替の技術としてだけIPが取り上げられているわけではありません。CDNやOTT、現場からのモバイル中継やFPUのIP化、PCによる編集システムや局システムなど、幅広い分野で既にIP技術が用いられています。電波で発射される放送波ですら、4K/8K放送からIPのフォーマットが採用されています。IP化のメリットが及ぶ範囲は同軸ケーブルからの乗り換えだけに留まりません。局のシステムやワークフローすべてがIPの上で稼働するようになるのです。

そういう観点では、IPを取り巻くエコシステムそのものの存在が、IPを選ぶ理由になるかもしれません。IP技術の発展は今後も続くでしょう。仮にSMPTEが新しいプロトコルを考案していたとしても、IPよりメリットがある、あるいは広範囲に使われる保証や確信がない限り、マーケットは支持しなかったかもしれません。

3.6 IPの応用例〜リモートプロダクション

IPのメリットを応用した例が「リモートプロダクション」という形で提案されています。遠隔地にあるベニュー(会場)からIPネットワークを用いて中継をしようというコンセプトです。現状では放送局は中継車とクルーをベニューに派遣して番組を制作しています。しかしこの手法では、例えばオリンピック・パラリンピックなど同時に複数のベニューで競技が実施されている場合、どうしても制約が生まれてしまいます。中継車の台数は限られていますので、その数に合わせて中継する競技を選択しなければなりません。

しかしカメラは既にリモートでの操作に対応しています。向きはリモート雲台で制御できますし、絞りやピント合わせは現状でも遠隔操作が主流です。現場のカメラマンは、カメラの向きしか意識していないことがあるのです。それ以外の操作は中継車の中でビデオエンジニアと呼ばれる技術者がモニタを見ながらカメラ機能を操作しています。それならばいっそのこと、カメラからの映像出力を直接IPネットワークに接続してしまえば良い。その映像をIPで運び、番組を制作している局舎内のサブスタジオに届けてしまおう。すると、ベニューに出向くクルー

を最小限にしてしまえる。大多数のスタッフはサブスタジオに詰めたまま番組制作が可能になるだろう、というわけです。

現在ではスポーツ中継には2～3台から多くて数十台のカメラが現場に設置されます。もちろん台数が必要とされるような競技では、引き続き中継車とクルーがベニューに派遣されることになるでしょう。しかし少ないカメラ台数でも競技の動きが追いかけることができ、かつ演出上の問題が少ないのであれば、リモートプロダクションの意義は高まると思われます。もちろん現場に十分な帯域を持つ光ファイバを引き込まなければなりませんが、現状でもメジャーなベニューにはその用意があることが多いです。この光ファイバを使ってEthernetとIPを運ぶようにすれば、潤沢な帯域のIPネットワークが現れます。放送局でもリモートプロダクションへの関心は高く、今後PoCや導入が活発になっていくでしょう。

3.7 本格化するPoCと案件

IIJでもVideo over IP技術の普及促進を加速すべく、2015年よりPoC(Proof of Concept)を実施してきました。IIJのバックボーンには100GbEの導入が進んでいます。帯域の観点では4Kの映像を数本流すことは問題ないと思われました。しかしVideo over IP技術に取り組み始めた当初は疑問がありました。汎用的なIP装置で構成されているIIJのバックボーンを用いて、ロスやディレイにセンシティブな4K映像を伝送することができるのか？

こうした疑問を解決するには、畢竟、試してみるほかありません。そこで、東京飯田橋のオフィスから大阪を経由して戻ってくる仮想ネットワークを構築しました。バックボーンとアクセス光ファイバ、そしてMPLSルータを用いています。このネットワークを流れるトラフィックはIIJの他のサービストラフィック

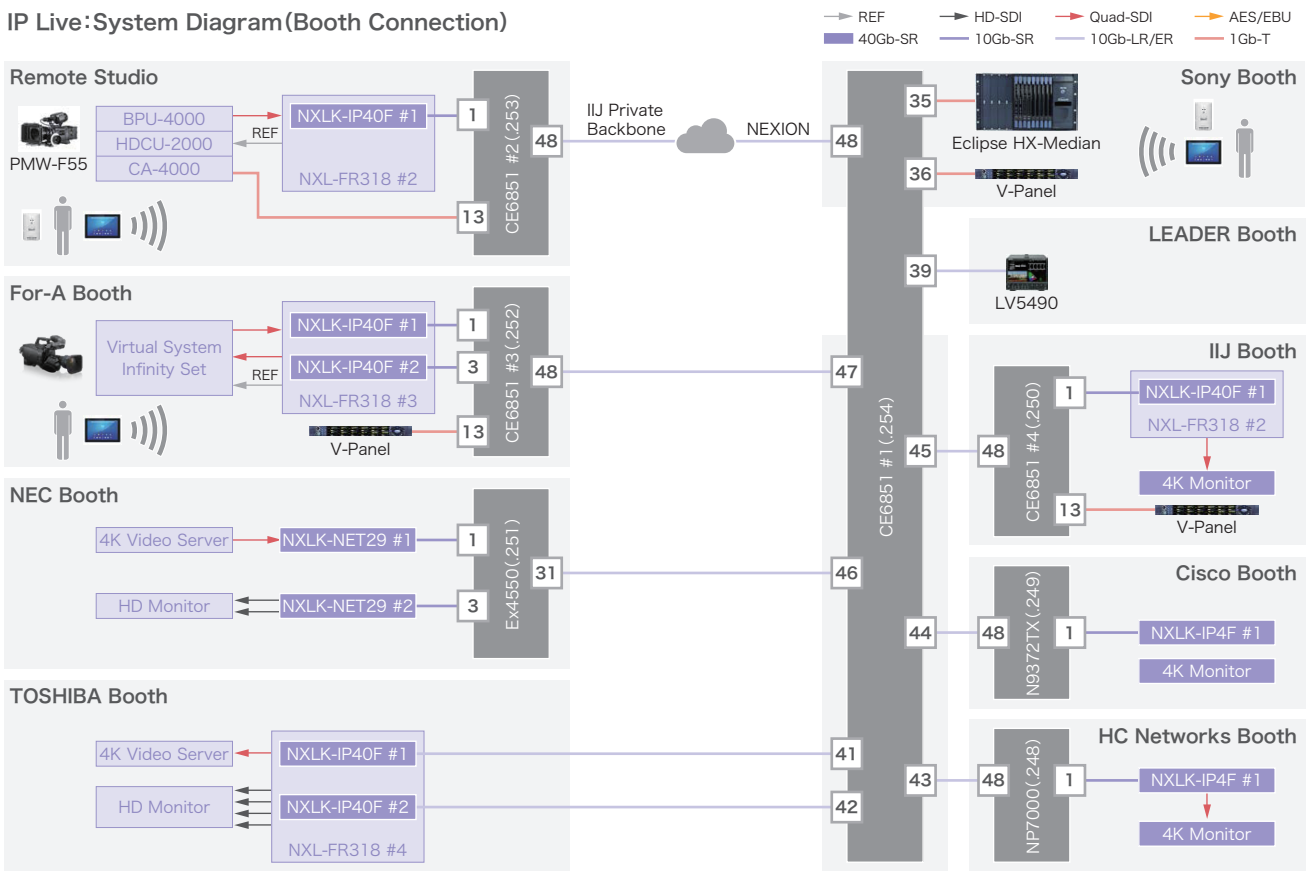

図-4 Inter BEE 2017におけるリモートプロダクションの例
IIJ飯田橋オフィスをベニューに見立て(図中左上)、幕張メッセのSonyブース、IIJブースとネットワークで接続する

とは区分されて転送されますが、下位レイヤーで用いている専用線の帯域は共有しています。完全に専用線で構築してしまってはコストが嵩むことと、IIJとしてバックボーンを用いない実験にはあまり興味がないためです。

そしてこの環境を用い、協力いただけるメーカ各社とPoCを進めてきました。HDもしくは4K映像を1本ないし複数本流すという実験がメインとしています。またメーカによっては更にPTPやAudio over IPの実験も同時に実施をしています。そしてこれらのPoCはほぼ問題なく成功を収めています。IIJでPoCを開始した頃はまだIPへの移行を確信している関係者はそう多くありませんでした。特にユーザは得体の知れないIPという技術に疑心暗鬼だったように記憶しています。こうした方々に新しい技術の可能性を説いて回っていた時期でしたが、この状況はしばらく続きました。

当初筆者は4Kへの対応がIP化のタイミングになると考えていました。4Kは単純計算でHDの8倍のデータ量があります(画素4倍、フレームレート2倍)。これは、4Kを導入した際にすべての区間の伝送路において必要となる帯域が8倍になることを意味します。HD向けに設計・構築された伝送路には、4K信号を伝送するだけのキャパシティがありません。新しく4K対応するための伝送路を設計したときに、IP技術の採用検討が進むのではないかと思われたのです。ところが欧米では、HDのVideo over IP化が盛んです。4Kを待つことなしにIPのメリットを享受しようという考えなのです。なぜ、と問うと「将来的にコストメリットにつながる」「4Kを待たず、今からIPに着手しておくべき」という意見が多いようです。もっともな話に聞こえますが、投資のタイミングを考えると微妙な感じもあります。この辺りは放送局の投資についての彼我の差があるのかもしれません。極端な話としては、IP化のメリットは？という自問に「Because we can」というスライドで答えたプレゼンテーションを見たことがあります。一種のジョークでしょうが、技術者らしい回答だなと感じました。

IIJはPoCにより経験を積むと共に、メーカとの知識共有を図っていきたいという狙いがあります。IPでできることを伝えると同時に、正確なナレッジとより質の高いノウハウを作り出していきたいからです。実際、広域ネットワークを使った実験の経験があるメーカはほとんどありませんでした。PoCで取得したデータはメーカにも提供し、フィードバックを実施しています。またエンドユーザにPoCを見学してもらうことも推進しています。実際のネットワークを使ったデモンストレーションは非常に効果的であり、セールス・マーケティング的にも大きな評価をいただいています。

時期	PoC内容
2015年7月	Sony IP Live。4Gbpsx2本を飯田橋→大阪→飯田橋へ伝送。Video over IP最初の試験となった。
2015年8月	Evertz ASPEN。4K甲子園の映像をグランフロント大阪から飯田橋へ伝送。
2016年6月	PFU QG70 + NTT-IT StreamMonitor。1.5Gbps HD映像を飯田橋→Interop会場へ伝送。
2016年10月	Sony IP Live。新規開発のモード検証。飯田橋→大阪→飯田橋へ伝送。
2016年11月	Sony IP Live。Inter BEE会場内でIIJブースとSonyブースを接続。
2017年2月	MediaLinks IP-VRS。HD/4K映像伝送実験。飯田橋→大阪→飯田橋へ伝送。
2017年6月	Sony IP Live。本格的な映像機材(リモートカメラ、オーディオコンソール)を含めたデモンストレーション。
2017年6月	Embrionix。映像IP変換SFPを用いたHD伝送。飯田橋→大阪→飯田橋へ伝送。
2017年6月	LAWO V__remote4 + セイコー TS-2950。HDおよび4K、64chマルチチャンネルオーディオ伝送。PTP相互接続実験。
2017年11月	NHK放送技術研究所。2017NHK杯フィギュアにて、大阪から東京への8K伝送実験をNHK技研が実施。 IIJはこの実験に対しプライベートバックボーンを提供(10GbE x 5本)。8KはDualGreen 24Gbps。

表-4 IIJにおける代表的なPoC

このようなPoCの成功には、全レイヤーのネットワーキング実践が必須です。当然、ネットワークレイヤーだけでなく映像、音声の技術的知識も必要とされます。PoCを数多く経験して感じていますが、機材を設置して、必要とされる設定を投入し、すべての結線を完了させても、最初はうまくいかないことがほとんどです。なぜ映像が届いていないのか、再生されないのか。様々な理由が考えられます。ルータやスイッチの設定ミス、バグ、トラヒック溢れ、コミュニケーションミス、誤解、などなど。起き得ることのすべてが発生すると思っておいて間違いがないほどです。それらを根気よく、1本1本捩れた紐を解きほぐしていく努力と時間が必要です。マルチキャスト技術の知識はもちろんIP、Ethernetなどのネットワーク知識、更には光ファイバケーブルの物理的特性など、エンジニアとして持てるナレッジを総動員させる必要があります。ケーブルの差し間違えで映像が映らないというのもよくある話です。PoCはトライ＆エラーの繰り返しですから、どうしても考慮洩れやミスが発生することは避けられません。こうした些細な点に気づくことができる資質も必要です。しかし、こうしたPoCで発生したミスやエラーは、すべてがこの後への「ギフト」です。

3.8 圧縮技術

4Kの場合、非圧縮映像の伝送には12G-SDIを必要とします。つまり12Gbpsの帯域が要求されるわけで、Ethernetの世界で普及している10GbE1本では送りきれません。そこで放送機器業界では25GbEへの移行というメッセージを出し始めています。これならば1本のネットワークインタフェースで4k非圧縮映像を送れるようになります。しかしこのメッセージが有効に働くにはもう少し時間がかかると思われます。イーサネットスイッチの25GbE対応とコスト低減にはもう少し時間がかかりそうだからです。

非圧縮映像は遅延や画質の面で優れているのですが、より多くの帯域を必要とします。そこで圧縮技術の導入によって、帯域の圧縮を図る動きがあります。この分野では既にいくつかの圧縮技術が登場しています。

- JPEG2000：既に標準化されている圧縮技術
- VC-2：BBC R&Dが開発し、SMPTE ST 2042として標準化されている
- LLVC：Sonyが開発。Low Latency Video Codecの略。SMPTE RDD 34として参考図書出版されている
- Tico：IntoPixが開発。現在JPEG-XSとして標準化作業中

これらの圧縮方式はどれも"Visually Lossless"と呼ばれています。圧縮を経てすべてのデータがそのまま取り出せる可逆圧縮ではありません。完全なデータはどうしても復元不可能な非可逆圧縮ではあるものの、「見た目には問題なし」というものです。（ですので厳密な意味での"lossless"とはいい難いのですが、一種のマーケティング用語でしょう。）この「問題がない」とはつまり、圧縮による画質劣化や遅延がその後の編集作業に影響を及ぼさないことを意味します。HEVCなどの高圧縮技術と異なり、「伝送のために軽く圧縮する」という意味合いで「軽圧縮」、非圧縮と高圧縮の中間にあるため「メザニン」などとも呼称されます。おおむね、4K映像の伝送レートを半分から1/4程度まで圧縮することを目的とした方式です。

こうした圧縮技術は各企業がパテントを所有していることもあり、標準化作業においてもそれぞれの思惑が影響するだろうと言われています。どの技術が標準規格になるか、あるいはどの規格をmandatory, optionalとするのかなど、様々な議論が戦わされる可能性があります。

3.9 事例と今後のVideo over IP技術の発展

前述したIP Showcaseでは回を重ねるごとに、実際の事例紹介が増えてきています。特に屋外での中継（Outside Broadcasting）に用いられるOB Van, OB Truckと呼ばれる中継車の内部ではIP化がかなり進行しています。中継車内の映像ネットワークは内部で一旦完結するからで、新しい技術を導入しやすいのです。日本でも既に中継車へのIP技術導入が進んでいます。

日本国内では2017年に入り大きなシステム構築案件の発表が続きました。Perform JapanはDAZNのデジタルライブスポーツプロダクションセンターのためにEvertzを採用しました。またSonyのIPルーティング設備は静岡放送やスカパーJSATなどに相次いで導入されています。

Video over IP技術の浸透やロードマップを描く動きもあります。The Joint Task Force on Networked Media(JT-NM)がそのような活動をカバーしています。このJT-NMはAMWA(The Advanced Media Workflow Association)、EBU(The European Broadcasting Union)、SMPTE、VSF(The Video Services Forum)による合同アクティビティで、リファレンスアーキテクチュアやロードマップを発刊しています。"JT-NM Roadmap of Networked Media Open Interoperability"は現状の位置付けと将来の技術発展を示すもので、業界内で広く共有されています。これによると現在は第1フェーズの「SDI over IP」と第2フェーズの「Elemental flows」が完成しつつある段階です。今後は第3フェーズの「Auto-Provisioning」と第4フェーズの「Dematerialized facilities」が控えています。Auto-Provisioningはリソースマネジメントのオートメーション化を目的としており、現在AMWAがワーキンググループを作り規格策定が進んでいます。

AMWAの活動はNMOS(Networked Media Open Specifications)として、以下の3つの策定が進んでいます。

- IS-04:Discovery and Registration Specification
- IS-05:Device Connection Management Specification
- IS-06:Network Control Specification

この中でも野心的なのはIS-06でしょう。

1. Discovery of Network Topology and Discovery of endpoint devices that are connected to the Network Switches
2. Create/Retrieve/Update/Delete Network Streams (Flow Management)
3. Monitoring and Diagnostics

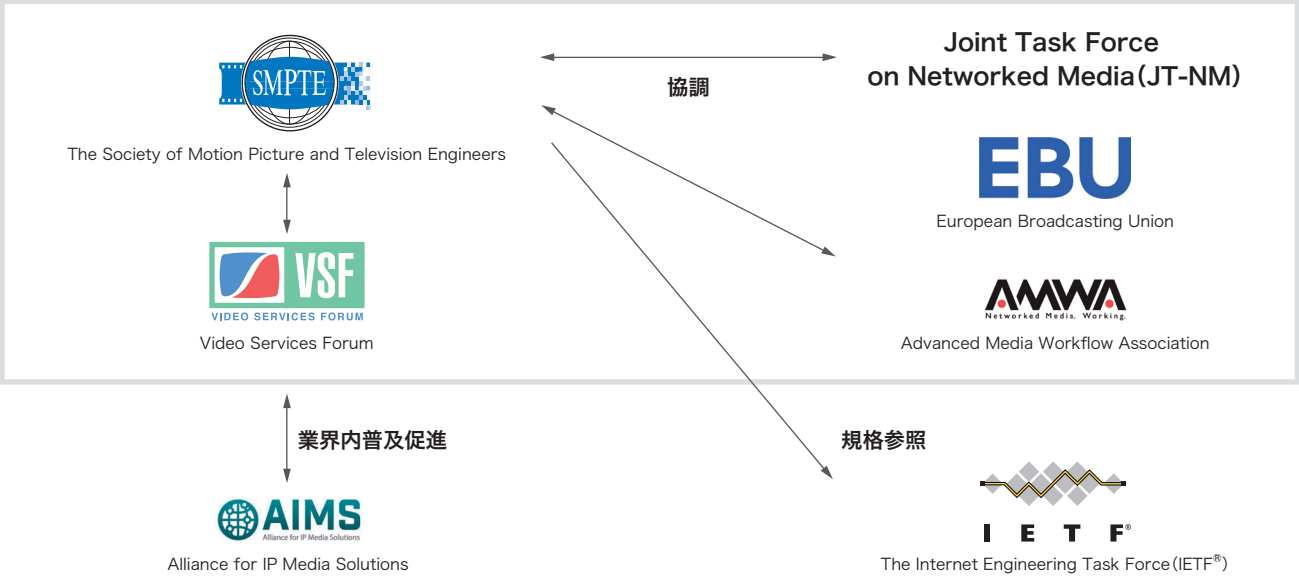

図-5 各標準化団体の関連

IS-06はこの3点の機能をカバーするものになる予定です(現状は1の部分に着手しているそうです)。主にコントローラからネットワーク装置に対するAPIに相当しますが、SDN的なアプローチと考えて良いかと思います。アプリケーション層からダイレクトにネットワーク層へとAPIでアクセスする発想そのものは、EvertzもSoftware Designed Video Networkというコンセプトで訴えていました。大きく異なるのは、IS-06は標準を狙っているということです。したがって多くのネットワーク装置メーカの賛同を得る必要があります。ARISTAは既にIBC2017で積極的な姿勢を見せていました。他のメーカもいずれ対応を明らかにしてくるでしょう。

AMWAの活動の中では、セキュリティについても問題意識が高まっているそうです。セキュリティについての討議がVideo over IP関連のどのコミュニティで成されるべきかはさておき、必要な議論には違いありません。

セキュリティが扱う範囲は非常に多岐に渡るため、どの分野をどのような観点でカットするかは今後の議論が必要になるでしょう。一例として、伝送されるIPデータの暗号化が挙げられるでしょう。閉域網を流れるデータだからといって暗号化をしなくても良い、とは限らないはずです。IPの世界ではIPsecと呼ばれる、汎用的にIPパケットを暗号化する仕組みがあります。またRTPに対して暗号を施すSRTP(Secure Real-time Transport Protocol)という規格もあり、どちらもRFCとして出版されています。しかしVideo over IPとしてどのような技術を採用するかは、まだまだ議論も始められていないようです。

IIJとしてこのVideo over IP技術をどう応用してマネタイズして行くかは、これからの検討課題です。バックボーンの利用はもちろんですが、データセンターあるいはクラウドとの結合が大きなテーマになると考えています。放送局からの発信がCDNやOTT、更にはハイブリッドキャストや4K/8K放送など

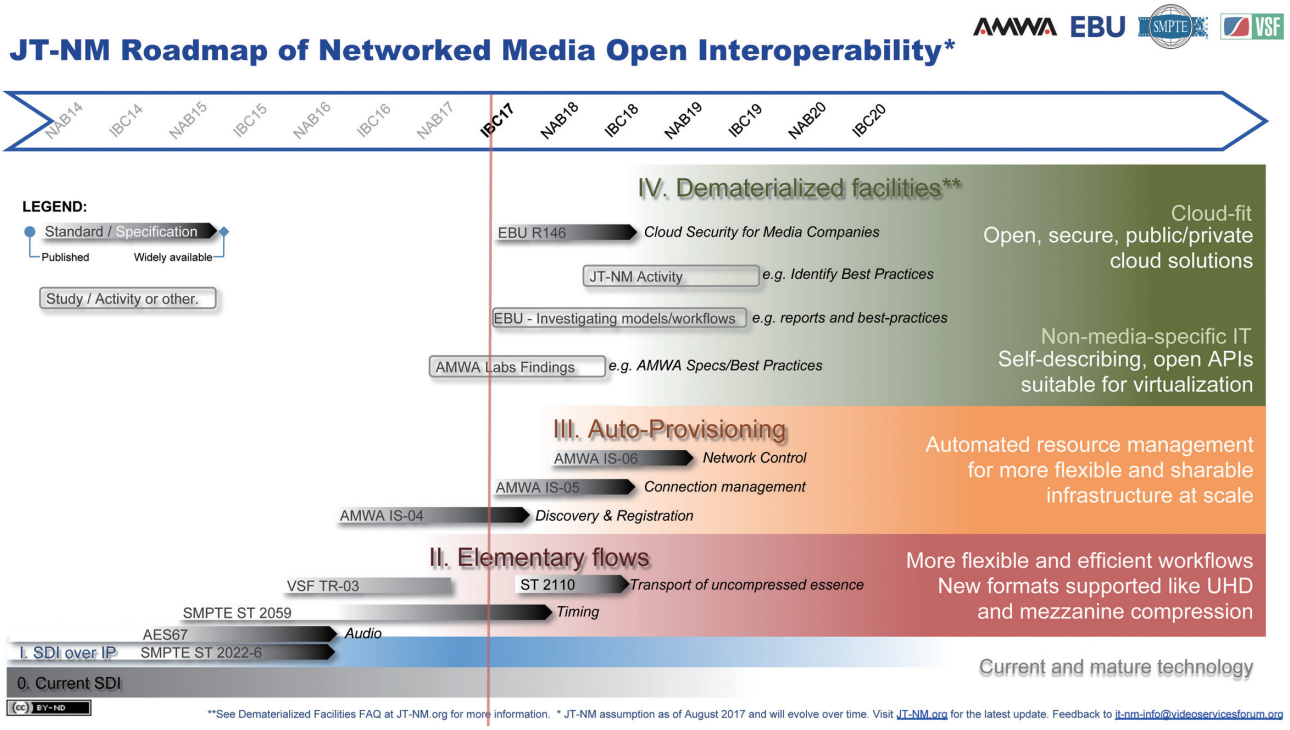

図-6 JT-NMによるJT-NM Roadmap of Open Interoperability(August 2017)*2

*2 Joint Task Force on Networked Media(JT-NM)(http://www.jt-nm.org/documents/JT-NM_Networked_Media_Roadmap_of_Open_Interoperability_1708-FINAL.pdf)。

によりどんどんIP化されていく中、Video over IPへの移行がどのようなメリットをもたらすかを、幅広く議論していくことになります。

また放送局にとってはIP技術の習得が大きなテーマになるでしょう。テクノロジーカンパニーとしての放送局業務において、IPは既に切っても切り離せない技術になっているはずです。映像の編集作業はビデオテープによるものから「ファイルベース」と呼ばれるPCソフトウェアによるものに替わってきています。ノンリニア編集ソフト(Adobe PremiereやApple Final Cut Proなど)を使うために、大容量のストレージと作業用のPCはネットワーク化されています。既に業務に深く入り込んだネットワークがあるわけで、IPの観点からするとVideo over IPは新しいアプリケーションに過ぎないとも言えます。いずれにせよIP技術の理解なしにVideo over IP技術の理解はなく、エンジニアとして習得すべきものとなっていくでしょう。

また、日本でも相互接続検証を立ち上げることが必要です。IIJでもPoCを通じて経験を蓄積していますが、これは広く共有されるべきものだと考えています。多くの参加者を募り、全員でひとつの目標のためにオペレーションする。案件ではないので大胆な設定も可能でしょうし、あれやこれや試してみることもできるでしょう。それには、こうした相互接続検証の場を設けることが一番です。そうした観点で、IIJでは「VidMeet」というイベントを開始しました。Video over IP技術について公開の場でのレクチャーやデモの機会はまだ限られているのが現状です。Video over IP市場はこれから熟成していく段階にあり、必要な人(ニーズ)に必要な人(知恵)が出会う必要があると感じています。ユーザとメーカ、ソリューションプロバイダとの出会い、実地デモ、そして議論ができる場を意図しています。

この初回イベントは「VidMeet1」として、2017年10月4日に第1回を開催しています。100名を超える参加者に対し3つのレクチュア及びデモンストレーションを実施しましたが、非常にポジティブな意見をいただきました。VidMeet2も2017年12月11日の開催を予定しており、引き続き積極的な参画をお願いしたいと考えています。

Video over IP技術は、技術が立ち上がる黎明期特有の期待感に溢れています。新しい技術の獲得と進展に心が躍り、エンジニアリングそのものが問われる。新しい業界の知己が増え、新鮮な気持ちでディスカッションできる。エンジニアとして、そんなエキサイティングな時間を過ごしています。

執筆者:
山本 文治(やまもと ぶんじ)
IIJ 経営企画本部 配信事業推進部 シニアエンジニア。
1995年にIIJメディアコミュニケーションズに入社。
2005年よりIIJに勤務。主にストリーミング技術開発に従事。同技術を議論するStreams-JP Mailing Listを主催するなど、市場の発展に貢献。

Intent-Based Network Security

4.1 はじめに

「Intent-Based Networking(IBN)」という言葉を聞いたことはありますか。あるベンダーが、ネットワークの設計や管理、運用のあり方を大きく変える製品展開を表明したことで一躍有名になりましたが、IBN自体はそれよりもう少し前から存在する概念で、特定の製品やソリューションを指す言葉ではありません。

従来のネットワークでは、ユーザあるいはネットワーク管理者が行いたいこと(意図)は、各種ネットワーク機器へ設定として記述されます。実際にネットワーク機器へ設定がなされるまでには、まず行いたいことをネットワーク機器が理解できる言語に変換し、更に変換したものをネットワーク機器に設定することが必要です。

後者に関しては、負荷を軽減する手段として、CLI(Command Line Interface)だけでなく、Web画面からの設定やネットワーク上から自動的にダウンロードするゼロタッチプロビジョニングなど、いくつかの方法が存在します。

しかし、前者のネットワーク機器が理解できる言語に変換することについては、ネットワーク管理者がネットワーク構成や用いる機器の特性を理解した上で自ら行う必要があり、モバイル環境やマルチクラウド環境が前提となる昨今は、その複雑さを増しています。

■ HowではなくWhatで

ユーザあるいはネットワーク管理者は自身が行いたいこと(what)だけを考え、それに応じてネットワークが自動的に構成される(how)としたらどうでしょうか。そして、さらにネットワーク自らが自身を監視・管理し、状況に応じて問題に対応してくれるとしたら、どうでしょうか。このようなことを実現しようという考えがIBNです。

4.2 IIJのIBN

IIJのIBNは、2012年に設立したIIJのグループ会社[*1]にて本格的に始まったSDN・NFV製品の研究開発の成果を基盤としています。図-1は、その基盤をもとにしたIBNの基本的なアーキテクチャ図です。ユーザがオーケストレータを介して「ネットワークに対して行いたいこと(what)」を設定します。それを「変換」し、Intent North-Bound Interfaceを用いてコントローラレイヤーに対して通知します。コントローラは、オンプレ側あるいはクラウド上に配置可能です。加えて、コントローラレイヤーは分散方式を採用しており、複数のコントローラが協調して動作し、コントロールレイヤーからネットワークインフラレイヤーにあるネットワーク機器やVNF(Virtual Network Function)に対して必要な設定(how)が行われます。VNFもまたオンプレ側とクラウド側のどちらにも配置可能です。Network Control Interfaceとしては、OpenFlowやREST APIなどを用いています。Intent North-Bound Interfaceとして、独自のAPIを実装しています。

IIJがIBNで具体的に実現しようとしているものは、ゼロ・トラスト環境を前提としたセキュリティの新しい仕組み「Intent-Based Network Security」です。

■ ゼロ・トラスト環境

BYODやIoTの普及により、企業ネットワークには様々な種類のデバイスが多数接続される環境となり、また、医療現場や製造業の現場などでも、様々な機器がネットワークに接続されるのが当たり前となっています。しかし一方で、それらのデバイスに必ずしも適切なセキュリティ対策を施せているかというとそうではありません。セキュリティ対策を実装するための十分なハードウェアリソースを持たないデバイスや、医療機器や産業用機器に組み込まれたソフトウェアなど、容易にはアップデートできないことがあります。そしてそもそも、何がいまネットワークに繋がっているか、が管理できていない環境も現

*1　プレスリリース「IIJとACCESS、次世代クラウド基盤技術の研究開発を行う合弁会社を設立」(https://www.iij.ad.jp/news/pressrelease/2012/0405.html)。

実には存在します。今日では、特定の組織や人をターゲットにした標的型攻撃も増加すると共に手口も巧妙化しています。つまり、現在の企業ネットワークにおいて安全と言い切れる環境は存在しない、と言えます。この考えに基づくのが「ゼロ・トラスト」を前提としたアプローチです。ユーザもデバイスもアプリケーションも、すべてが無条件で信頼されることはなく、信頼しない代わりに常に検証することによって安全を確保しようという考え方です。

■ ポリシーベースセグメンテーション

何か障害が発生したとき、その影響範囲をできる限り小さくするために用いられる考え方をマイクロセグメンテーションと言います。マイクロセグメンテーションは、セグメント化する対象によっていくつかの種類に分けることができますが、IIJでは、以下の2つの考え方(ポリシー)をベースにし、同じポリシーを適用できるモノの集合をセグメントとする「ポリシーベースセグメンテーション」を用いています。

- ユーザ、デバイス、サーバ、PC、アプリケーションなどをすべて同等に扱う、すべてが「ネットワークにつながる何か(モノ)」だという考え方
- 「このモノと接続可能なモノはどこの何か」を設定する

例えば、Aさんがaプロジェクトとbプロジェクトに属している場合は、1つのモノに対して複数のポリシーを適用することも可能なので、それぞれのプロジェクト用のセグメントに所属することができます。つまり1つのモノが複数セグメントに属すことも可能です。

このポリシーベースセグメンテーションが、IIJのIBNの中心的な考えとなるものです。モノとモノをどう繋げるかということだけを考えさせる仕組みであり、ネットワーク管理者にとってシンプルかつ直感的に扱うことができます。

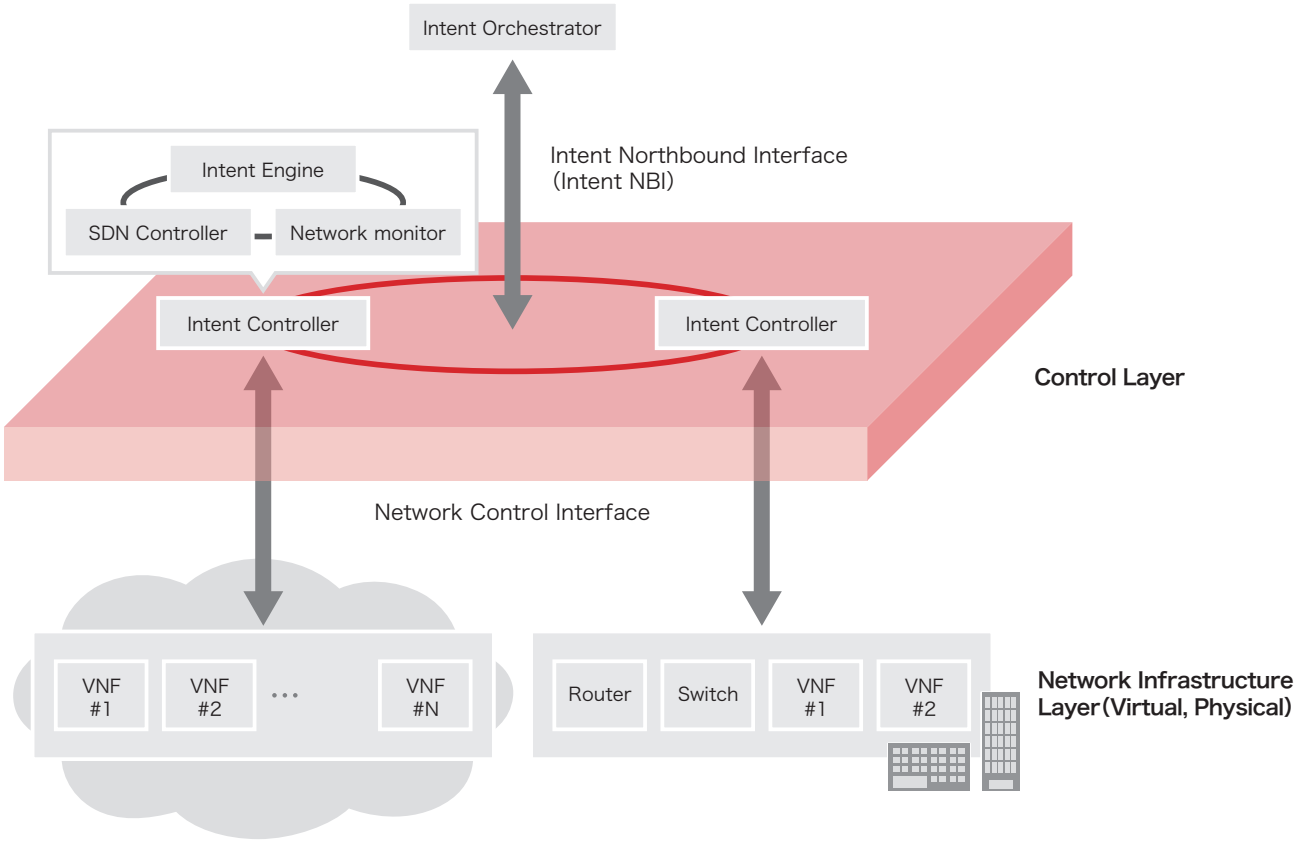

図-1 IBNの基本的な構成

■ IDとロケータの分離

従来は、IPアドレスにIDとロケータという2つの意味を持たせて利用していました。IPアドレスは、経路制御に用いられるようにロケータ（居場所を示すもの）である一方で、アプリケーションなどの上位層からみると、セッションを特定するためのIDとしても扱われています。しかし、IPアドレスが2つの意味を持つことによって、不便な状況となることがあります。例えば、ユーザ・端末がネットワーク間を移動した場合には、端末の IP アドレス（IDとロケータの両方）が変更され、元のIPを識別子として用いていたセッションが切れてしまいます。本来なら、単に移動しただけであればロケータとしての情報のみが更新されればよく、IDとしての役割の方には影響がないことが望ましいはずです。

そもそもネットワークセキュリティとして管理者が管理したいものはIPアドレスそのものではなく、誰がどの情報資産にアクセスできるのか（アクセスさせないのか）、といったレベルのことだけのはずです。後述しますが、IIJのIBNでは、ロケータやIDとしてIPアドレスを管理することを止めることによってこの問題を解決しています。

■ 開発コード「FSEG」

Intent-Based Network Securtyとしての取り組みは、開発コード「FSEG」として鋭意開発中です。FSEGの構造を前述したIBNの基本構造に照らし合わせて示したものが図-2です。ゼロ・トラスト環境における「監視と検証」そして「ポリシーベースセグメンテーション」の実現手段としてSDN技術を採用しています。

FSEGは、FSEG Controller、セキュリティVNF群を中心として構成されるオーバーレイ・ネットワークです。FSEG Controllerは、クラウド上に配置、あるいは、オンプレ環境ではFSEG

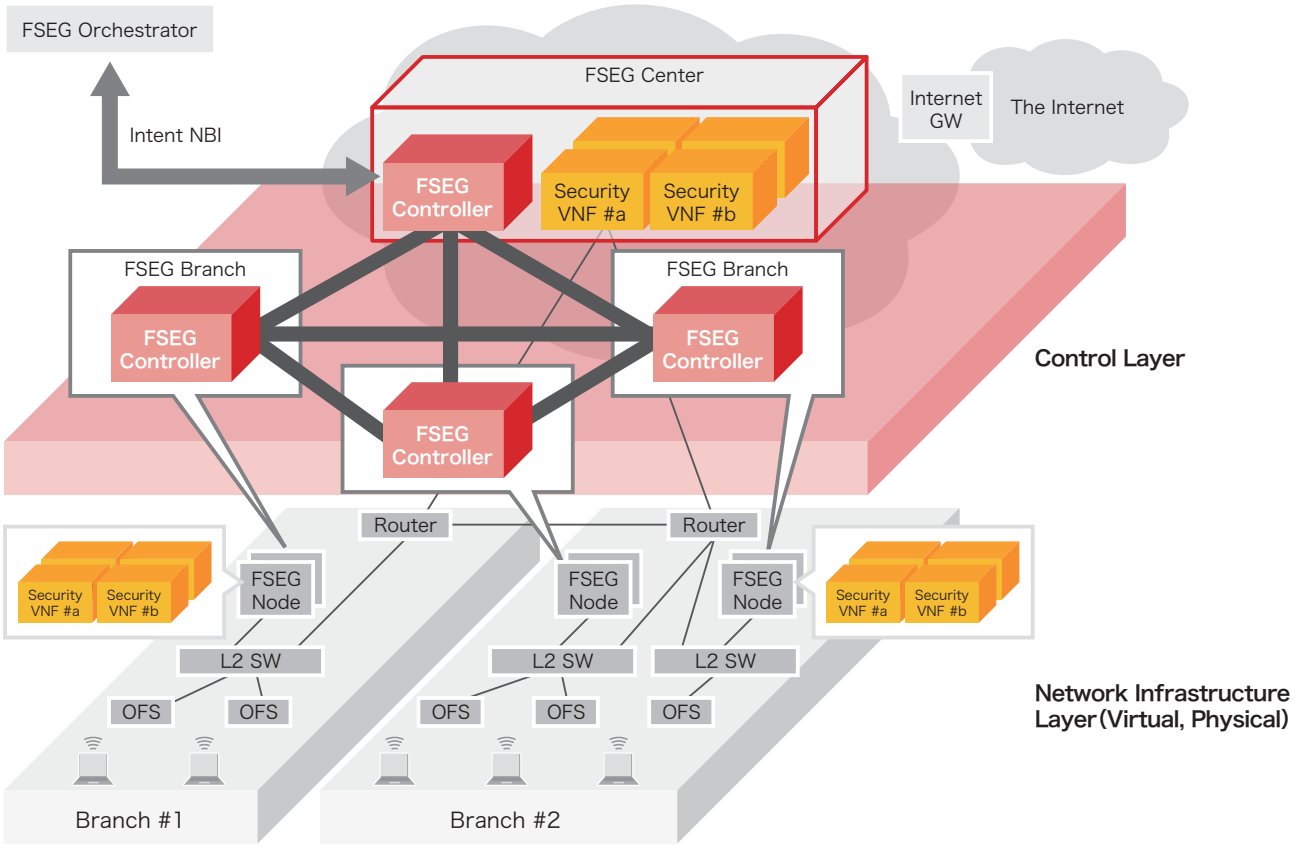

図-2 FSEG概観

Nodeと呼ぶ(小型)PCサーバ上に実装されることをイメージすると分かりやすいでしょう。FSEG Controller間はフルメッシュのL3トンネルで結ばれます。FSEG Controllerの主な機能は3つで、「ユーザ・デバイスの認証機能」「ポリシー制御(そのモノがどのFSEG Controller配下に接続可能か)」「(FSEG Nodeに搭載の)セキュリティVNF群の制御機能」です。

FSEG NodeにはFSEG Controllerの他にセキュリティVNF群が搭載されており、Active-Stanby構成での冗長化が可能です。アンダーレイとしては、OpenFlowスイッチをユーザとの接点とし、FSEG Nodeを中心としたネットワークを想定しています。

■ 監視と検証、セグメント

FSEG内に配置されるOpenFlowスイッチでは、配下のデバイス間の直接通信(スイッチからみればポート間通信)を禁じています。すべてのトラフィックは上位のFSEG Nodeへ転送され、すべてのデバイス間通信はFSEG Node経由で可能になります。これは、トラフィック監視をFSEG Node(上のFSEG Controller)にて実施するためです。また、FSEG Node(上のFSEG Controller)は、ポリシー制御の機能も有しており、「このモノ(人やデバイス)が接続可能なモノは何か」というポリシー情報を収容したデータベースを持っています。そのため、トラフィックごとにポリシー(接続可能先情報)を適用させる(接続先を制御する)ことが可能となります。このようにFSEG Nodeでトラフィックごとに接続先を制御することでセグメンテーションを構築しています。このように構成されるセグメントは、従来のVLANのように、ネットワーク機器の設定によるセグメントではなく、「モノ」を識別して構成するセグメンテーションです。

FSEGは、既存のネットワークとの親和性の高さも特徴の1つです。FSEG環境内では、IPアドレスはあくまで「モノ」と「モノ」をつなげるためのアンダーレイ技術として、(FSEG外とは)独立したIPアドレス体系を用います。FSEG NodeはDHCPサーバを内包していますので、直接FSEG環境を利用する「モノ」はこのDHCPサーバよりIPアドレスを取得します。一方で、FSEG Node配下のOpenFlowスイッチ内でNAT機能も実装しており、既存ネットワーク配下のデバイスがFSEG環境を利用する場合には、このNAT機能によりFSEGの中と外のIPアドレスを自動で書き換えます。したがって、このときに「モノ」自体はIPアドレスの変更を意識する必要はありません。FSEG NodeのDHCPサーバによるIPアドレス払い出しにせよ既存ネットワークで用いられていたIPアドレスにせよ、「モノ」にどのようなIPアドレスが払い出されたかはFSEG Nodeにて管理しFSEG Controllerの制御下に配置できますので、FSEGを利用するすべての「モノ」をセグメント対象とすることができ、ポリシー適用も可能です。このように、既存ネットワーク環境とFSEG環境は容易に共存でき、まずは検証から、といったスモールスタートのニーズにも応えられます。

4.3 ネットワーク全体を覆うセキュリティセンサー

「Intent-Based Network Security」であるFSEGは、新たなセキュリティ基盤を提供可能とします。それは、従来の「侵入防止」の考えではなく、現在の組織ネットワークに適した「早期検知と拡散防止」を目指したセキュリティセンサーの構築です。

■ モノの認証

まず、ポリシーベースセグメンテーションの要素となる「モノ」を特定するための手段ですが、FSEGでは様々なデバイスを想定して以下のように複数の認証の仕組みをサポートしています。

- IIJ ID(多要素認証)
- アカウント + パスワード(Web認証)
- MACアドレス認証
- 時間帯認証
- ロケーション認証(OpenFlowスイッチに接続の場合に、どのスイッチに接続されるか、による認証)
- 上記の組み合わせ

認証の成否を含めて、時刻／ユーザ名／MACアドレス／ロケーション(スイッチ)／IPアドレスを履歴管理します。

■ 全エリアで脅威情報を共有

前節で述べたように「モノ」からのトラフィックはすべてFSEG Nodeを経由させており、FSEG Node上のFSEG Controllerはそれらトラフィックを自身の配下のセキュリティVNF群による検査対象とします。また、FSEG Node内のFSEG Controller間はフルメッシュで接続されており、あるFSEG Controller配下で脅威が検知された場合は、その情報をすべてのFSEG Controllerで共有する仕組みを持っています。各FSEG Controllerは、自身の管理下にあるセキュリティVNF群の有効・無効の制御や、どのトラフィックにどのセキュリティVNFをどのような順で適用させるか(サービスチェイニング)を制御しています。これらの仕組みによって、あるFSEG Controller配下で検知された脅威をトリガーにして、関連するすべてのセグメント下に存在するFSEG Controllerにてセキュリティ VNFの追加・変更などを行ったり、ネットワーク設定を変更して脅威が検出されたセグメント全体を隔離したり、といったことが可能になります。つまり、ネットワーク全体を覆うセキュリティセンサーによって全トラフィックを監視し、それらからの情報をもとにネットワークがon-the-flyで形を変えることができるわけです。同じ仕組みで、オンプレとクラウド間での負荷分散・機能分散も実現します。例えばIPS機能をオンプレ側に配置しておいて、処理が間に合わなくなればクラウド側に新たにIPS機能を配置し負荷分散する、といったことが実現できます。

■ 予防的措置

ポリシーベースのセグメントは、「同じポリシーを適用できるモノの集合」であり、会社を例にすると、社内の同じ業務用サーバに接続する同じ部署内のユーザ・デバイス群のような場合です。ある部署で見つかった脅威は、見つかった時点で既に同部署内に拡散してしまっている可能性が疑われます。FSEGでは、セキュリティセンサーで見つけた脅威情報をもとに、そのモノが属するセグメントのポリシーを変更することで、そのセグメントに対して予防処置を施すことが可能になります。脅威が見つかったセグメントごとにトラフィック監視の監視レベルを引き上げたり、それまで適用していなかったセキュリティVNFを適用させたり、といった処置を動的に実施でき、推測される被害を最小限にしようとします。

■ ネットワークセキュリティを中心に

先にも述べましたが、IoTデバイス自体にセキュリティ対策が施されていることは必ずしも期待できません。政府の働き方改革の推進もあり、今後はオフィス環境を快適にするためにも多くのIoTデバイスがオフィスに入り込んでくることでしょう。それらが単体動作で完結することはなく、必ずデバイス外との通信が発生します。ネットワーク側でセキュリティの施策を行い、単なる脅威検知だけではなく脅威を排除する仕組みが必要となります。すべてを「モノ」として扱い、ネットワーク全体としてセキュリティを確保し、予防措置も可能とするFSEGは、IoT環境にも適しています。

4.4 今後

IIJのIBNへの取り組みにおいて、強みは2つあります。まずは、早くからSDN技術をベースとした製品の研究・開発を開始し、特にエンタープライズ領域においては他社に先駆けて独自のSDNソリューションを提供してきた実績やノウハウをベースにしていることです。例えば、本稿で説明したようなポリシーベースのセグメントに用いるトラフィック制御などに活用しています。そしてもう1つは、エンタープライズネットワークの新たなセキュリティの仕組みを提供する、という具体的なユースケースを明確に設定したことです。その結果、パートナー企業の協力も得やすく、ここで紹介した方法で実装が既に行われ、PoCも完了しています。

■ CPEとスイッチ

ユースケースと同時に検討すべきことは、提供の仕方です。IIJのソリューションとして提供するにあたり、お客様側へ設置するCPEとしてのFSEG Nodeをどのように設計・実装するかを検討しなくてはなりません。先述したように、その配下のトラフィックすべてがFSEG Nodeを経由することでFSEGの基

本的な仕組みが動作します。これはつまり、FSEG Nodeにトラフィック処理の負荷が集中することも意味します。この懸念を、3つのアプローチで払拭しています。1つには、必ずしもFSEG Nodeを経由しなくても良い仕組みを構築します。配下のOpenFlowスイッチと連携してフローごとにFSEG Node経由の要否を判断します。2つ目は、高負荷時に自動的にFSEG Node自身がスケールアウトする仕組みです。最後にハードウェアアクセラレーションとしてDPDKやASICなどの技術を利用します。今後はこれらを組み合わせ、お客様に最適な形態として提供できるように準備していきます。

なお、今回はFSEG Node配下にOpenFlowスイッチを配した構成で説明しましたが、必ずしもOpenFlowスイッチは必要ではありません。その場合は、FSEG Nodeに「モノ」が直接つながる形態となり、今回説明したOpenFlowスイッチが担っている機能(「モノ」間の直接通信を禁止するなど)をFSEG Nodeにて実装します。

■ SOCとの連携

Intent-Based Network Securityを実現するFSEGを更に強化するには何が必要でしょうか。ネットワーク全体を覆うセキュリティセンサーであるFSEGは、センサー群からデータを収集することができます。そしてFSEGは、何をしたいか(what)からhow(どう実現するか)に変換できます。ここで不足しているのは、大量のデータをもとにしてwhatを定めてあげることです。これは換言すれば、「収集した大量のデータを保持し知見によってそれらを分析でき、活用できること」でしょう。IIJでは、セキュリティへの取り組みとしてwizSafeブランドも立ち上げました。セキュリティオペレーションセンター(SOC)も稼働しており、膨大なデータを分析し、知見を蓄積しています。これらとFSEGを連携させ、より強固で洗練されたセキュリティ基盤とすることを検討しています。

■ 最後に

お客様は行いたいこと(what)だけを意識すれば良く、その実現方法(how)はIIJが担うという考え方は、実はIIJが以前から取り組んできたものでもあります。今回は、SDN、NFV技術をベースとしたIBNへの取り組みとしてFSEGをご紹介しましたが、例えば、これまでにIIJが開発してきたSMF[*2]、SACM[*3]、Omnibus[*4]などもその考えを具現化したものです。連綿と受け継がれる思いは変わらず、しかし常に最新の技術で具現化していくという姿勢で、FSEG開発を続けて参ります。

執筆者:
水野 正和(みずの まさかず)
IIJ ネットワーク本部SDN開発部シニアプロダクトマネージャ。
株式会社ストラトスフィア時代からSDN・NFV技術をベースにしたプロダクト開発及びビジネス開発に従事する。

＊2　SMF(SEIL Management Framework:エスエムエフ):2006年3月に特許取得(特許第3774433号)。
＊3　SACM(Service Adaptor Control Manager:エスエーシーエム):「SMFv2(日本:特許第4463868号、米国:特許7660266号)」の自動接続、完全管理の仕組みをOEM提供するための、マネージメントサービス基盤。SMFv2は「SEILシリーズ」だけでなく、他社のネットワーク機器に対しても、初期設定から設定変更、運用管理までを一元的に管理できる。
＊4　Omnibus:SDNとNFVの技術を活用したクラウド型の新しいネットワークサービス(https://www.iij.ad.jp/omnibus/)。

December 2017 Vol.37

Internet Initiative Japan

株式会社インターネットイニシアティブ(IIJ)について

IIJは、1992年、インターネットの研究開発活動に関わっていた技術者が中心となり、日本でインターネットを本格的に普及させようという構想を持って設立されました。
現在は、国内最大級のインターネットバックボーンを運用し、インターネットの基盤を担うと共に、官公庁や金融機関をはじめとしたハイエンドのビジネスユーザに、インターネット接続やシステムインテグレーション、アウトソーシングサービスなど、高品質なシステム環境をトータルに提供しています。
また、サービス開発やインターネットバックボーンの運用を通して蓄積した知見を積極的に発信し、社会基盤としてのインターネットの発展に尽力しています。

株式会社インターネットイニシアティブ

〒102−0071 東京都千代田区富士見2-10-2　飯田橋グラン・ブルーム
E-mail : info@iij.ad.jp　URL : https://www.iij.ad.jp