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。

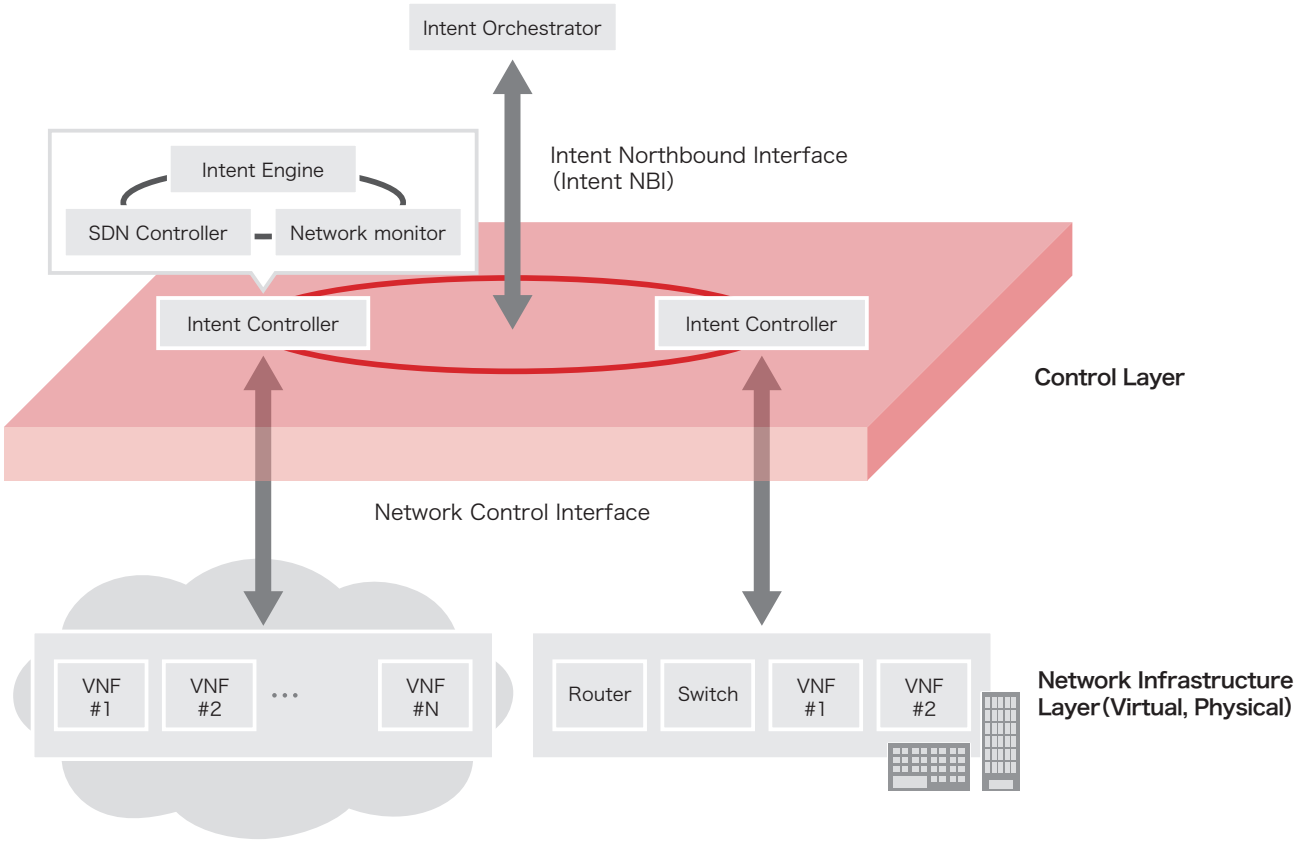

図-1 IBNの基本的な構成

■ 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

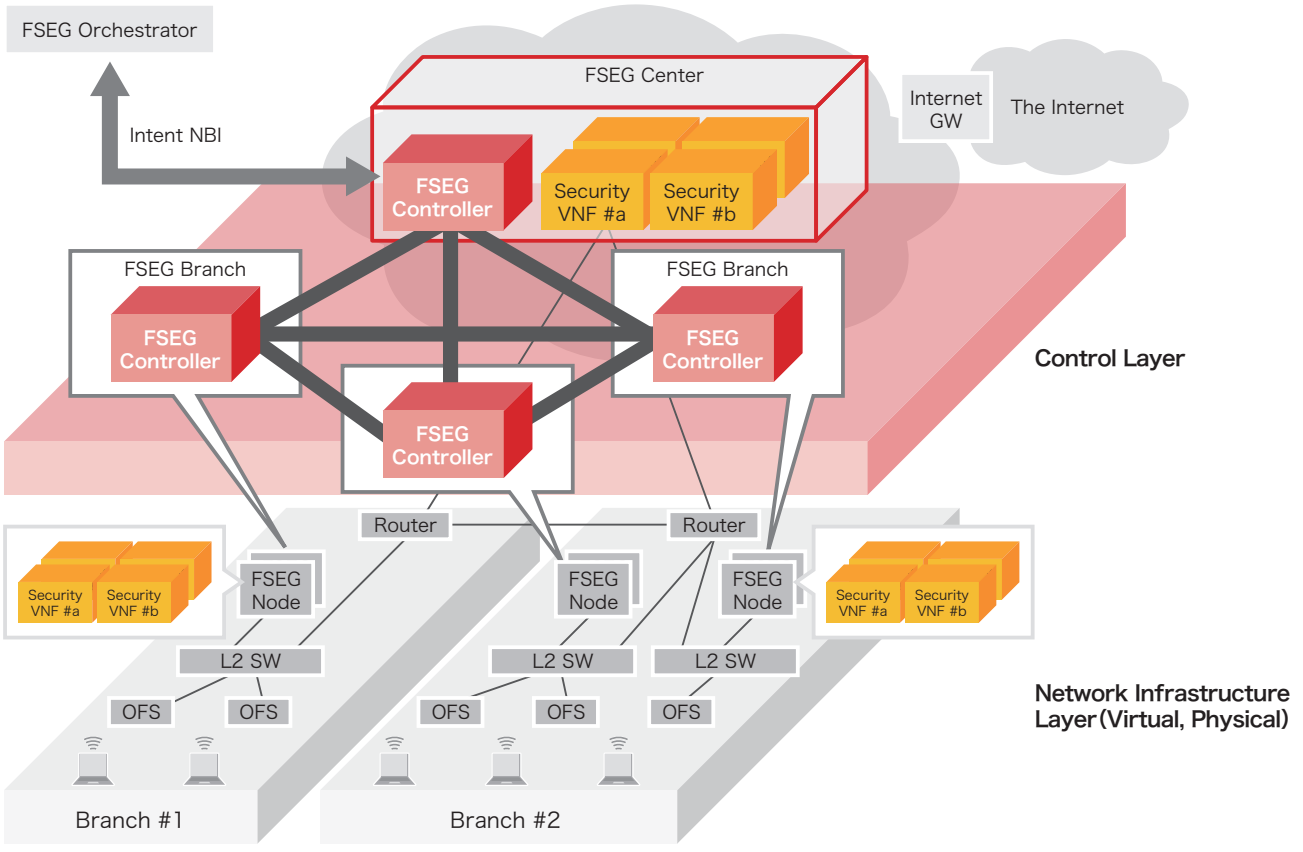

図-2 FSEG概観

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/)。