IIJ Internet Initiative Japan

IIJ Omnibus SD-LAN/WAN で目指すSDNの世界

2016年11月9日

(株)インターネットイニシアティブ
SDN開発部　白崎博生

Ongoing Innovation

Omnibus SD-LANとSD-WAN

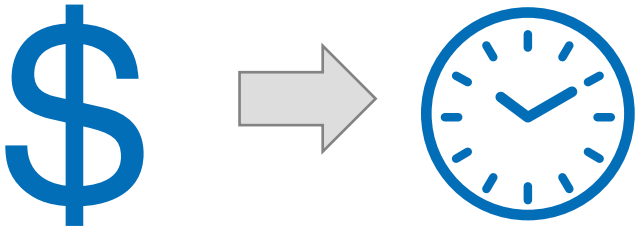
IIJ Omnibus SD-LANのサービス内容と来年度に向けて準備中の内容を解説し、さらにSD-LAN/WANの未来像についてお話します

第1部
SDN の基本的な考え方

SDN 登場の背景

SDN登場の背景: クラウド利用スタイルの変化

利用目的の変化



コスト削減からビジネス・アジリティへ

クラウドサービスの拡大

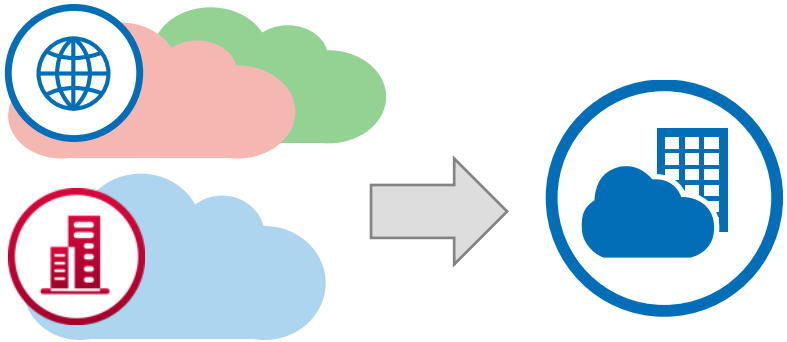
IIJ GIO
Office 365
box
salesforce
amazon web services™
Microsoft Azure

マルチクラウド環境へ

ユーザ意識の変化

単なる仮想化環境から、必要なものを必要なだけ(クラウドのツール化)

形態の変化

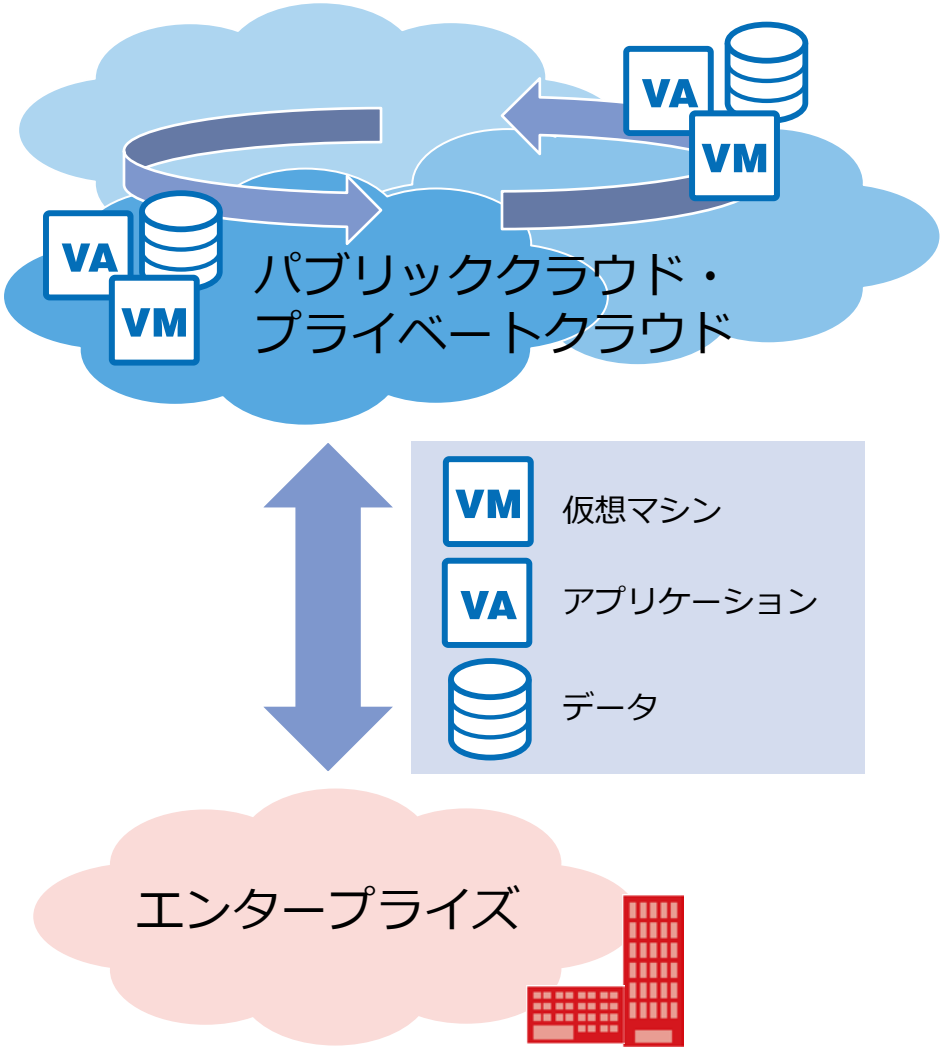


プライベートやパブリックから、
ハイブリッドクラウドへ

IoT 市場の急成長

様々な特性をもつ膨大なデバイス数

SDN登場の背景: 新たなネットワーク技術への要望



強い需要

- クラウドと協調するネットワーク
- 動的に生成される仮想環境へ対応可能なネットワーク
- 全方位 (North-South, East-West) のトラフィックをコントロール可能なネットワーク

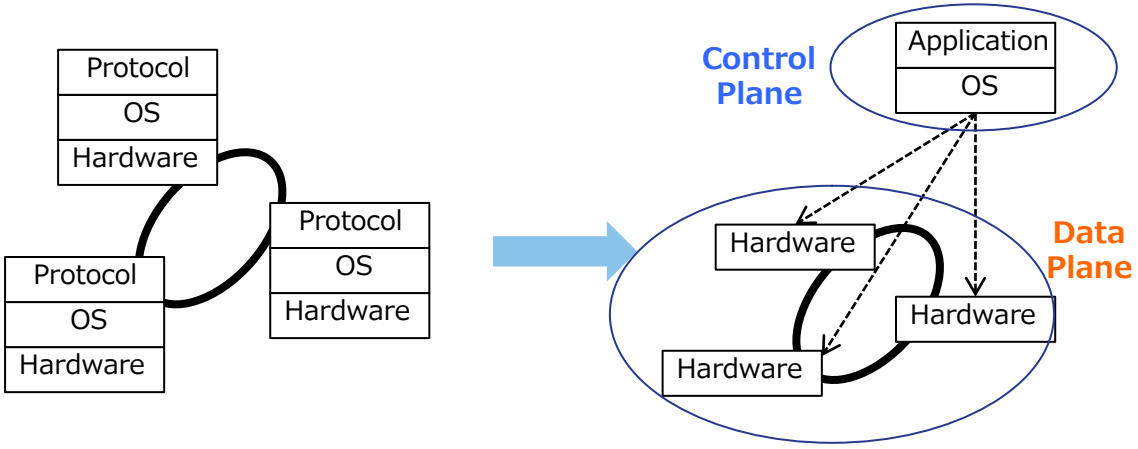
Software-Defined Networking (SDN) の登場

SDN の考え方

SDN とは

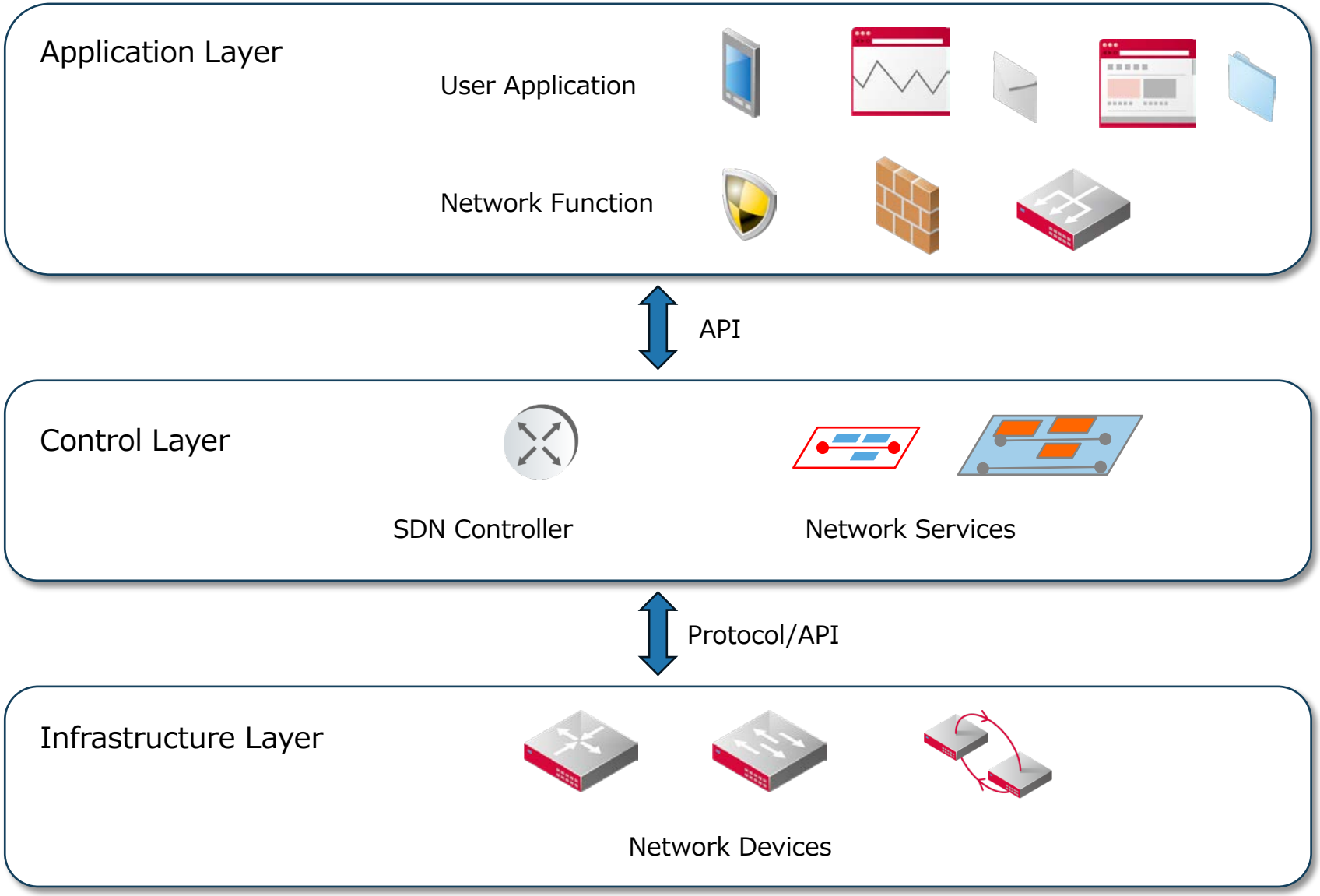
- 基本的な考え方
  - ネットワーク制御とデータ転送処理を分離
    - SDNコントローラによる集中型制御
      - 仮想ネットワークの設定や制御を行うには、多くの機器の設定や制御を協調させて実施する必要アリ。人手では非常に困難
  - SDN 自体はコンセプト。特定のプロトコルや機器を指すものではない

物理ネットワークにとらわれずに論理的なネットワークが構築可能



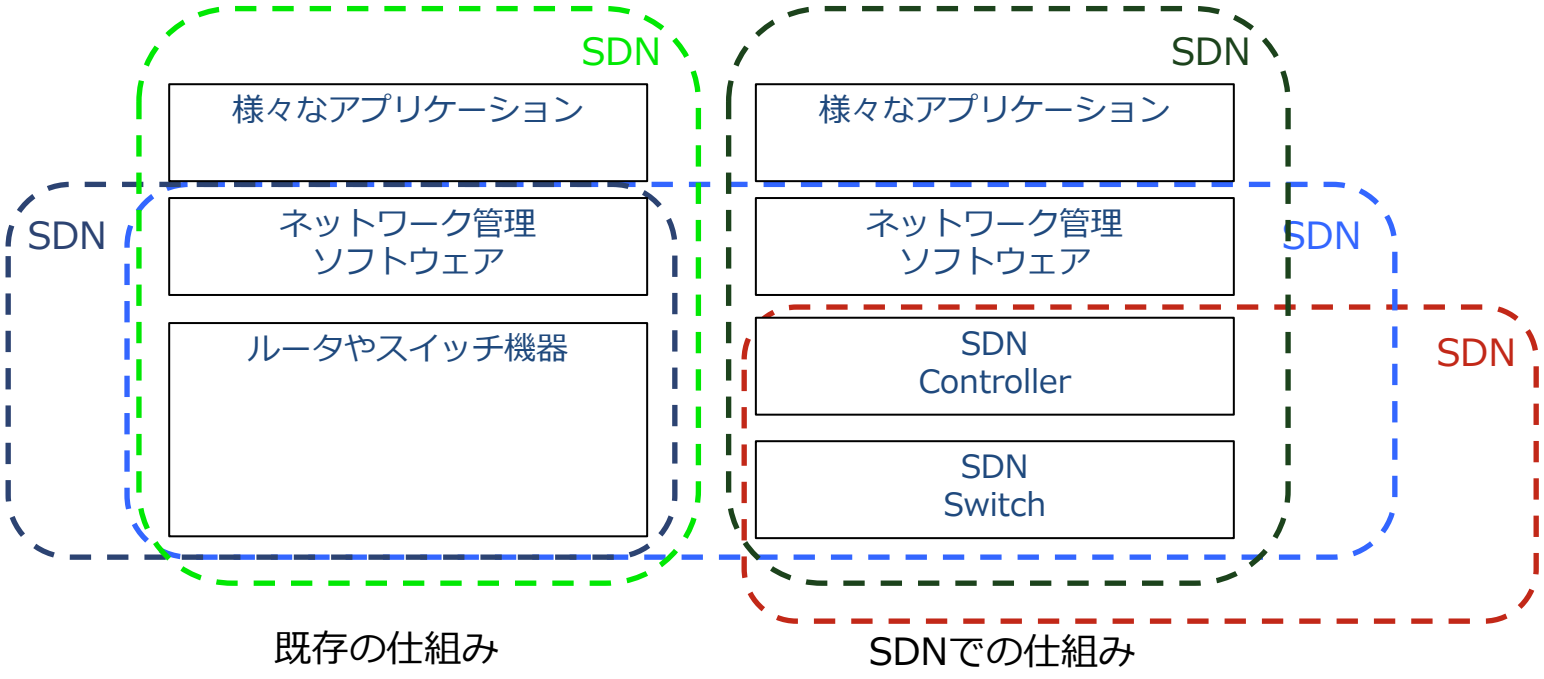
今まで　　SDN

SDN 基本アーキテクチャ



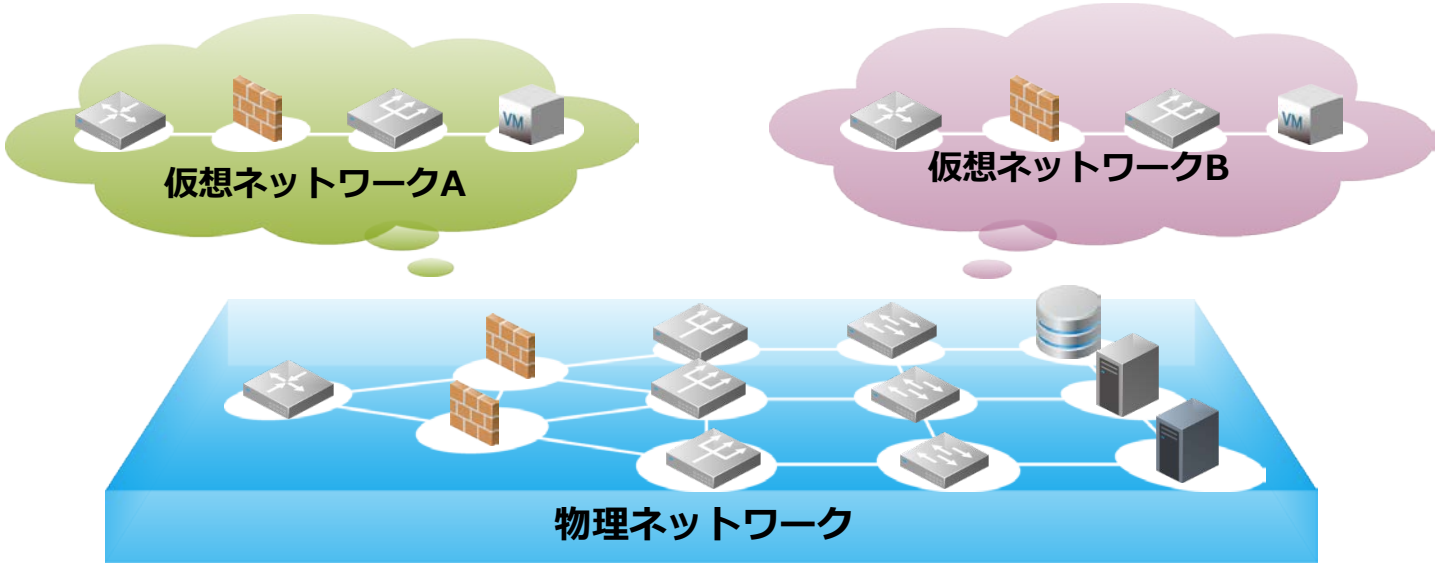
様々なSDN

- SDN 自体は単なるコンセプトであるため、用語としてはベンダごとに様々な用いられ方をされている



SDN の基本的な考え方 まとめ

- SDN はコンセプト
  - 特定のプロトコルや機器を指すものではない
- ネットワーク制御(コントローラ)部分とデータ転送部分を分離
- 物理的なネットワーク構成にとらわれず、論理的なネットワークが構築可能



第2部
企業ネットワークへのSDN導入

企業ネットワークの課題

エンタープライズWANの課題

異なるトラフィック特性を持つネットワークを接続する必要

- 基幹業務系
- インターネット接続系
- 音声・画像系
- IoT

クラウド、データセンタ、モバイル利用の増大によりトラフィックパターンは変化するのが当たり前の状況に

品質とコスト

- 過度な冗長化、低い帯域利用率
- セキュリティと回線コスト

業務アプリのクラウド化による、通信性能の問題も表面化

既存技術の課題

- トラフィック振り分けのための ECMP は、ハッシュ計算による偏り、振り分け先の帯域不足などが課題に
- PBRによる経路制御では、機器ごとにそのポリシー設定が必要。制御対象が増えるほど複雑化し、メンテナンス性が落ちる

エンタープライズLANの課題

利便性とセキュリティ確保の両立が困難

背景：
- オフィス統合などによる、組織形態の頻繁な変更
- 情報資産へのアクセス管理が、様々な雇用形態／業務内容に対応できていない
- 多様化するサイバー攻撃、標的型攻撃の増加
- タブレットやスマートフォンなどのモバイル端末の爆発的な普及
  - ✓ 社員による個人端末の持ち込み

課題：
- 複雑化、煩雑化したネットワーク
- ネットワーク機器に縛られた管理運用
- いつ誰が、どこから何を使ってアクセスしているかわからない。管理しきれない
  - ✓ 不正オペレーション、不正プログラムの侵入、情報漏洩時の追跡ができない
- 端末上でのセキュリティ確保(アンチウィルスソフト等) だけでは社内セキュリティとして不安
  - ✓ ユーザ利便性を犠牲にしたセキュリティシステムの導入

企業ネットワークへのSDN導入の意義

企業へのSDN導入の意義

1．企業ネットワーク構築・運用における生産性の向上

今まで	SDN
• 煩雑化したネットワーク • 組織変更や、サービス追加などのたびにNW機器の設定変更や配置変更、場合によってはケーブル再配置も必要に • ICT要員不足	• OpenFlow等の新技術により、NW機器の構成管理、稼働管理、障害管理、アカウント管理、セキュリティ管理を自動化・集中化 • NW構築や運用を従来より少ない人員で実施可能に • 人為的ミスや手戻りも軽減

2. 柔軟かつ迅速なネットワークサービスの投入

今まで	SDN
• 専用ハードウェアであるNW機器に縛られたサービス提供 • 複雑になったネットワーク全体を把握することが困難	• 汎用ハードウェア上へのソフトウェアによる機能展開と遠隔からの集中した設定管理 • 柔軟かつ迅速にネットワークサービスを拡張したり新規投入が可能に

企業へのSDN導入の意義

3. ネットワークインフラ運営上のリスクの低減

今まで	SDN
• 多種多様なNW機器に対しての、機能追加・変更時の負荷 ✓ セキュリティ対策の実施漏れなどの懸念も • 災害時やバースト的な負荷発生時などに柔軟に対応できない固定されたネットワーク	• 機器の設定管理やソフトウェアの展開、ユーザや端末認証が自動化され、ネットワーク状態やユーザアクティビティの可視化が実現可能に • 障害によるネットワークダウンの回避や、セキュリティインシデント発生の余地を少なくすることが可能に

4. CAPEX/OPEXの削減

今まで	SDN
• 専用ハードウェアの増加、 ✓ 消費電力の増加にも • 非効率な回線契約 ✓ 平常時には使用しないバックアップ回線など • 複雑化するネットワークの管理運用コストの増大 ✓ 過度なベンダ依存にも	• スイッチやサーバの物理的な台数の削減や、汎用機器への機能統合による導入機器の最適化と導入コストの低減、さらに、消費電力や冷却コストの低減が可能に • 回線の有効活用 • 管理・運用の自動化により人的リソースの最適化も可能となるため、コスト全体の最適化ができる

第2部: 企業ネットワークへのSDN導入 まとめ

- 企業ネットワークの課題
  - クラウド環境に対応できないネットワーク
  - ビジネス環境の変化に対応できない硬化したネットワーク
  - ネットワーク管理の複雑化に伴う管理コストの増大
  - 時代遅れのセキュリティ対策

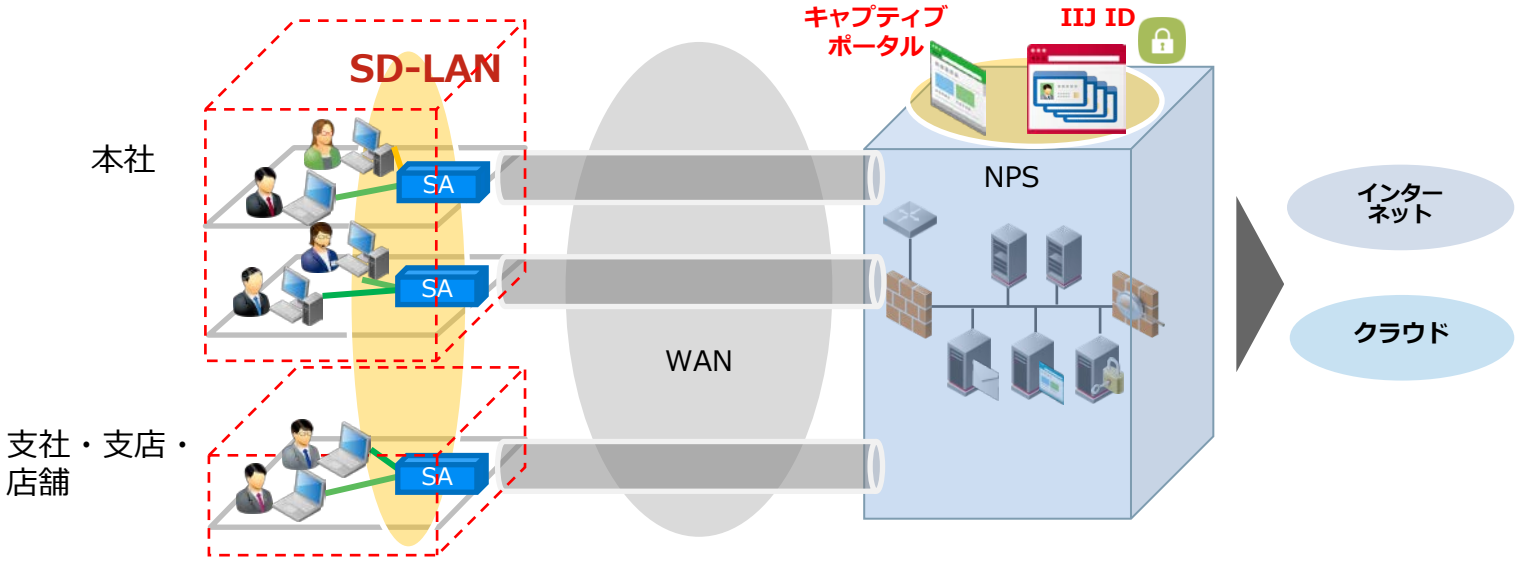
- 企業ネットワークへのSDN導入意義
  - 企業ネットワーク構築・運用における生産性の向上
  - 柔軟かつ迅速なネットワークサービスの投入
  - ネットワークインフラ運営上のリスクの低減
  - CAPEX/OPEXの削減

第3部
Omnibus SD-LANとSD-WAN

Omnibus SD-LAN

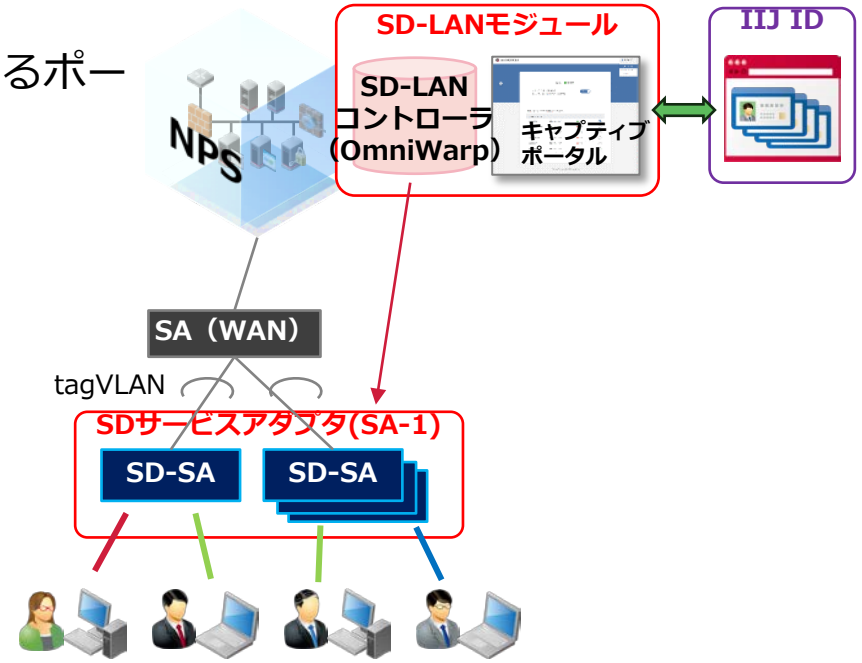
Omnibus SD-LAN

- **WebUI の操作で仮想ネットワーク作成**
- **ポリシーと認証結果に基づき、ユーザ（端末）を適切な仮想ネットワークに接続**
  - アカウント認証、MAC認証、アカウント＆MAC認証
- **IIJ-ID 連携**
  - ネットワークとアプリケーションの SSO
- **認証ログと接続ログ**
  - 「誰が」「いつ」「どのスイッチ」の「どのポート」から「どの仮想ネットワーク」に接続（切断）した



Omnibus SD-LAN システム構成

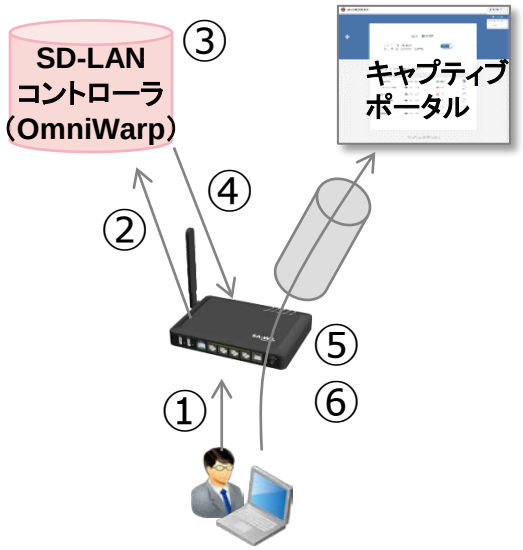
- **SD-LANコントローラ**
  - スイッチ設定をコントロール（OpenFlow 1.3）
  - ポリシーＤＢ
  - REST API
- **キャプティブポータル**
  - エンドユーザが仮想ネットワークを選択するポータルページ
  - ユーザ認証はIIJ-IDを利用
- **IIJ-ID**
  - ユーザ認証、SSOシステム
- **SD-LANコンパネ**
  - 仮想ネットワーク管理WebUI
- **Omnibus ポータル**
  - SD-LAN契約
  - 拠点契約
- **サービスアダプタ（ＳＡ）**
  - 無線AP
  - OpenFlow 1.3 スイッチ



SD-LAN の動作

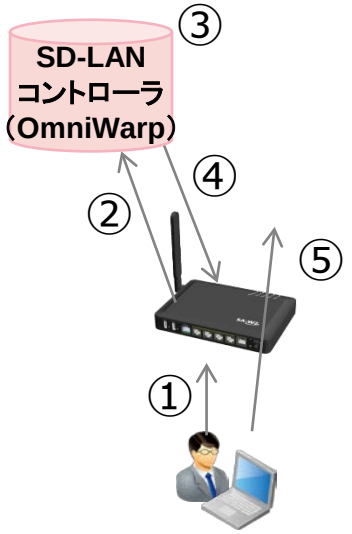
■ 仮想ネットワークを選択するまで

① ユーザがSAにパケット送信
② コントローラに PACKET IN
③ 認証状態を確認
④ ユーザの通信はVXLANトンネルを通すルールを登録
⑤ キャプティブポータルにログイン
⑥ 仮想ネットワークを選択



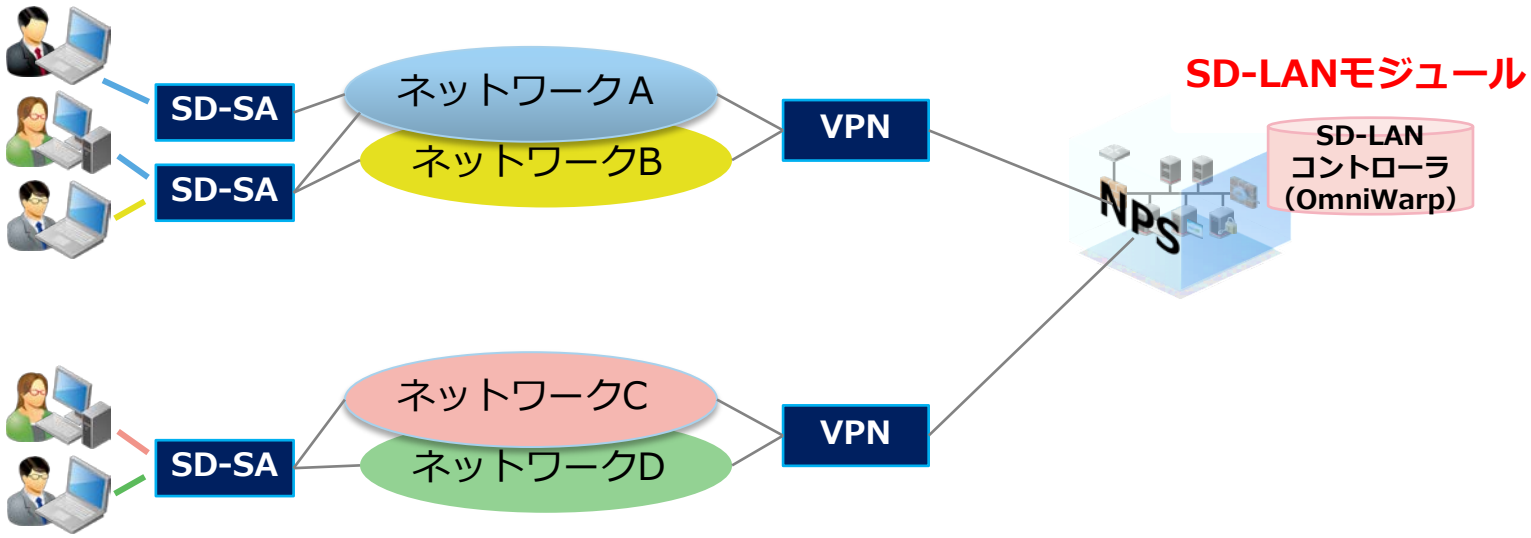
■ 仮想ネットワークの選択後

① ユーザがSAにパケット送信
② コントローラに PACKET IN
③ 認証状態を確認
④ ユーザの通信にVLANタグを挿入するルールを登録
⑤ VLAN 通信



Omnibus SD-LAN の仮想ネットワーク

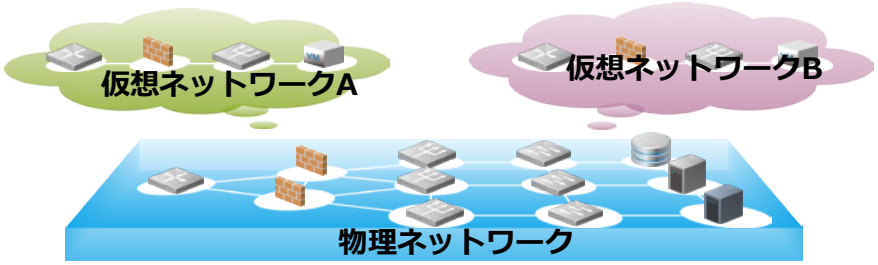
- **「拠点」の中に tagged VLANによる仮想ネットワークを作成**
  - 「拠点」内に作成できる最大数は○○
  - 仮想ネットワーク間ルーティングは拠点内のL3SWで行う（SD-LAN 制御外）
  - 仮想ネットワークのDHCPはWANモジュールのSAに設定、またはお客様に用意いただく



それだけ？

何をやりたいのか、どうしたいのか

- **自由にネットワークを作りたい**

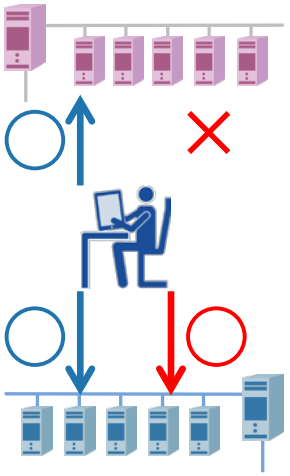


- **接続ポリシーの設定を容易にしたい**

平常時と非常時でアクセス可能なネットワークを変更
(ユーザ権限の変更)

平常時

機密情報に
アクセス可能



災害時

災害対策・復旧業務
に必要な場所のみア
クセス可能に

何が問題なのか

- **IP アドレスは使いにくい**
  - ID（識別情報）
  - 位置情報
  - ポリシー情報

  } IPアドレスは３つの情報を持っている

- **ネットワーク作成時に見積もる必要がある**
  - 現在と将来の割り当て数
  - アドレスブロック管理と経路表

- **冗長化**
  - 迂回路、ループ回避
- **ファイアウォールのルール**
  - ルールのスパゲッティ
- **ネットワークオタクがどこにでもいるわけじゃない**

IPブロックの割り当て例

現在

- 余裕を見越して割り当てる

本社	支社１	支社2	拠点1
192.168.0.0/17	192.168.128.0/20	192.168.144.0/20	192.168.240.0/24
			
192.168.0.0/24～ 192.168.127.0/24	192.168.128.0/24～ 192.168.143.0/24	192.168.144.0/24～ 192.168.159.0/24	

こうありたい

			
192.168.1.0/24 192.168.2.0/24 192.168.6.0/24	192.168.3.0/24 192.168.8.0/24	192.168.4.0/24 192.168.7.0/24	192.168.5.0/24

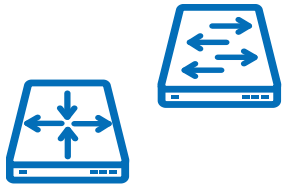
割り当てた順

理想のネットワーク

- **ネットワークは「誰が誰とお話ししてよい（お話しできない）」を実現できればよいはず**
  - これがネットワークの目的
  - IP は手段

- **個々の「誰」にポリシーを設定するのは面倒**
  - 管理対象のグループ化 → 仮想ネットワーク

- **他のことはオタクと機械が考えればよい**
  - IPアドレスアサイン、最適経路、迂回経路、フィルタルール等
  - 位置情報からの解放

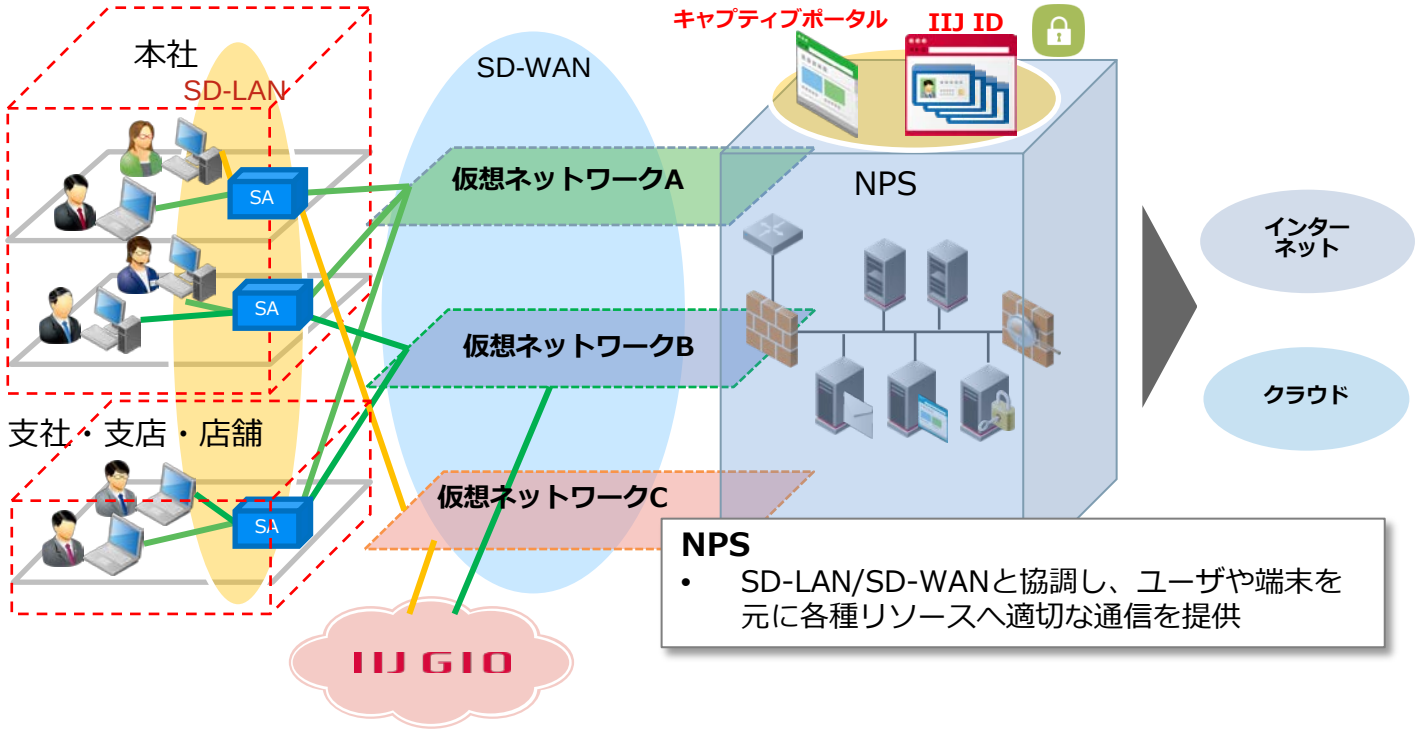


- **オーバレイとアンダーレイ**
  - 目的の実現 → オーバレイ
  - 手段の実現 → アンダーレイ

Omnibus SD-WAN

Omnibus SD-WAN

- 自由にネットワークを作るシステム
  - 一般的な SD-WAN 製品とは異なります
- オーバレイ型の仮想ネットワーク
  - 拠点間を擬似 L2 接続
  - 管理対象を減らすことが目的
- 仮想ネットワーク間のルーティング
- 特定端末のパケット操作
  - ねじまげ、コピー、書き換え等
- 接続先
  - オンプレ、DC、GIO P2、他社クラウド
- VNF 配置とサービスチェイニング
  - パターン化/メニュー化
- フィルタリング
  - ファイアウォール
  - VLAN間ルータ
  - サービスアダプタ
  - フィルタをかける場所をユーザは意識しない



第3部: Omnibus SD-LAN/SD-WAN まとめ

- Omnibus SD-LAN
  - ポリシーと認証結果に基づき、ユーザ（端末）を適切な仮想ネットワークに接続
  - IIJ-ID とも連携

- Omnibus SD-WAN
  - オーバレイ技術で、拠点間を仮想L2ネットワークで結ぶ
  - 仮想ネットワーク間のルーティング
  - フィルタリング

第4部
SDN ユースケース:
次世代セキュリティ

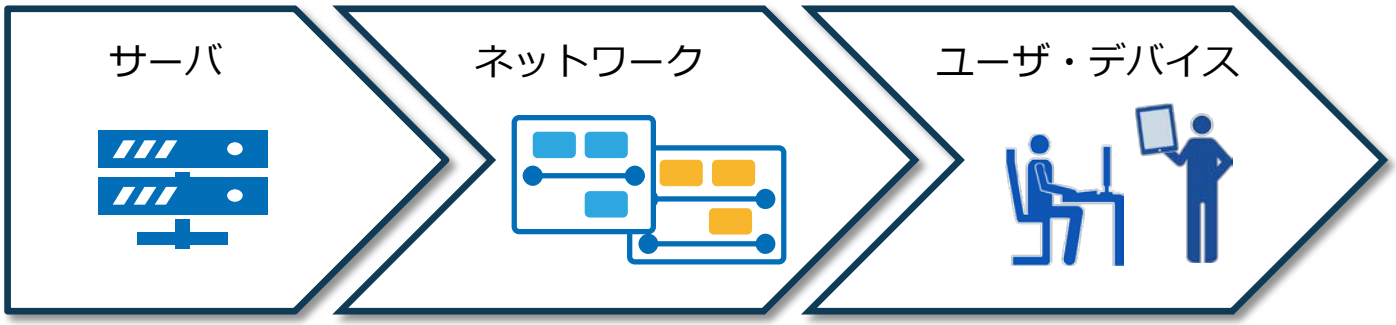
企業でのセキュリティ運用

企業のセキュリティ運用

企業のセキュリティ運用に求められる対応

- 被害範囲の迅速な特定
- 被害の最小化
- 速やかな原因解析と復旧

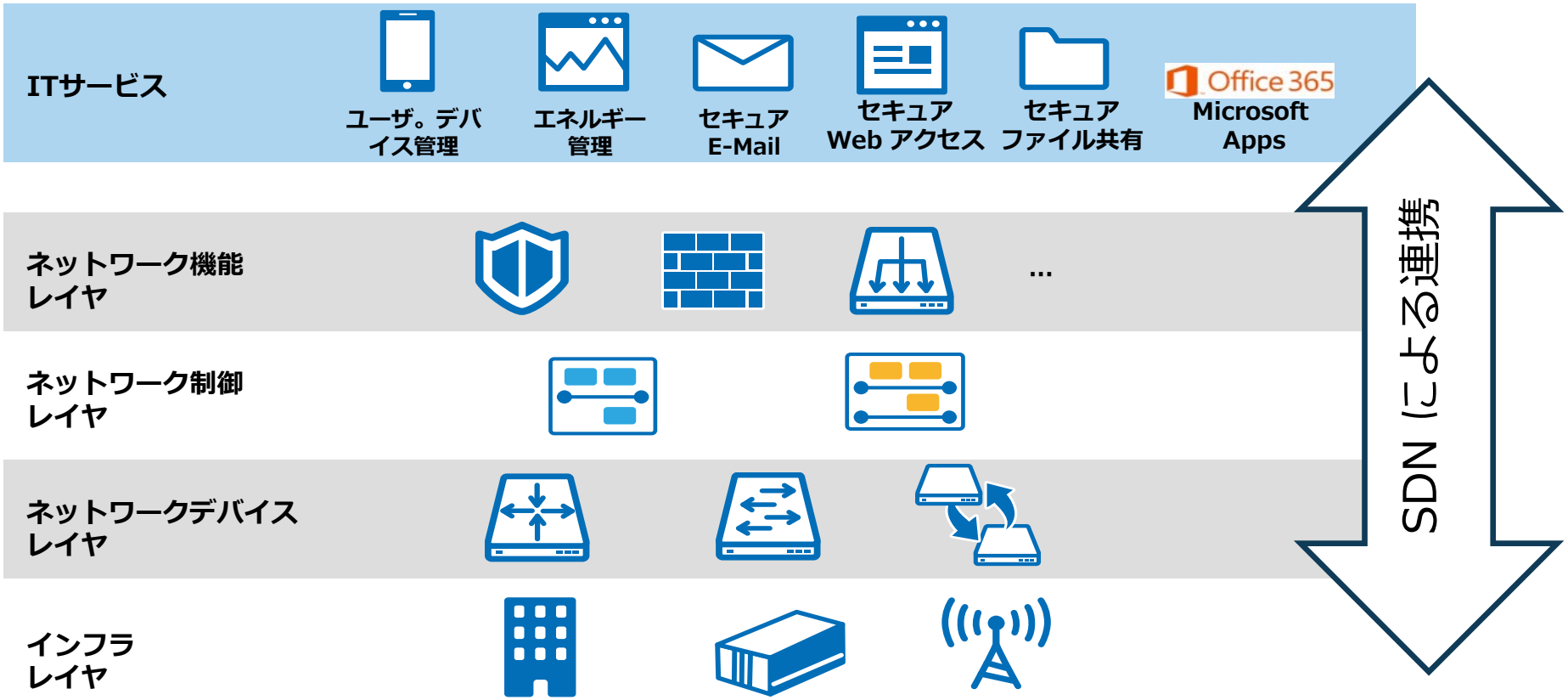
今の時代、多層防御だけでなく連携したセキュリティが必要



次世代セキュリティ環境の構築

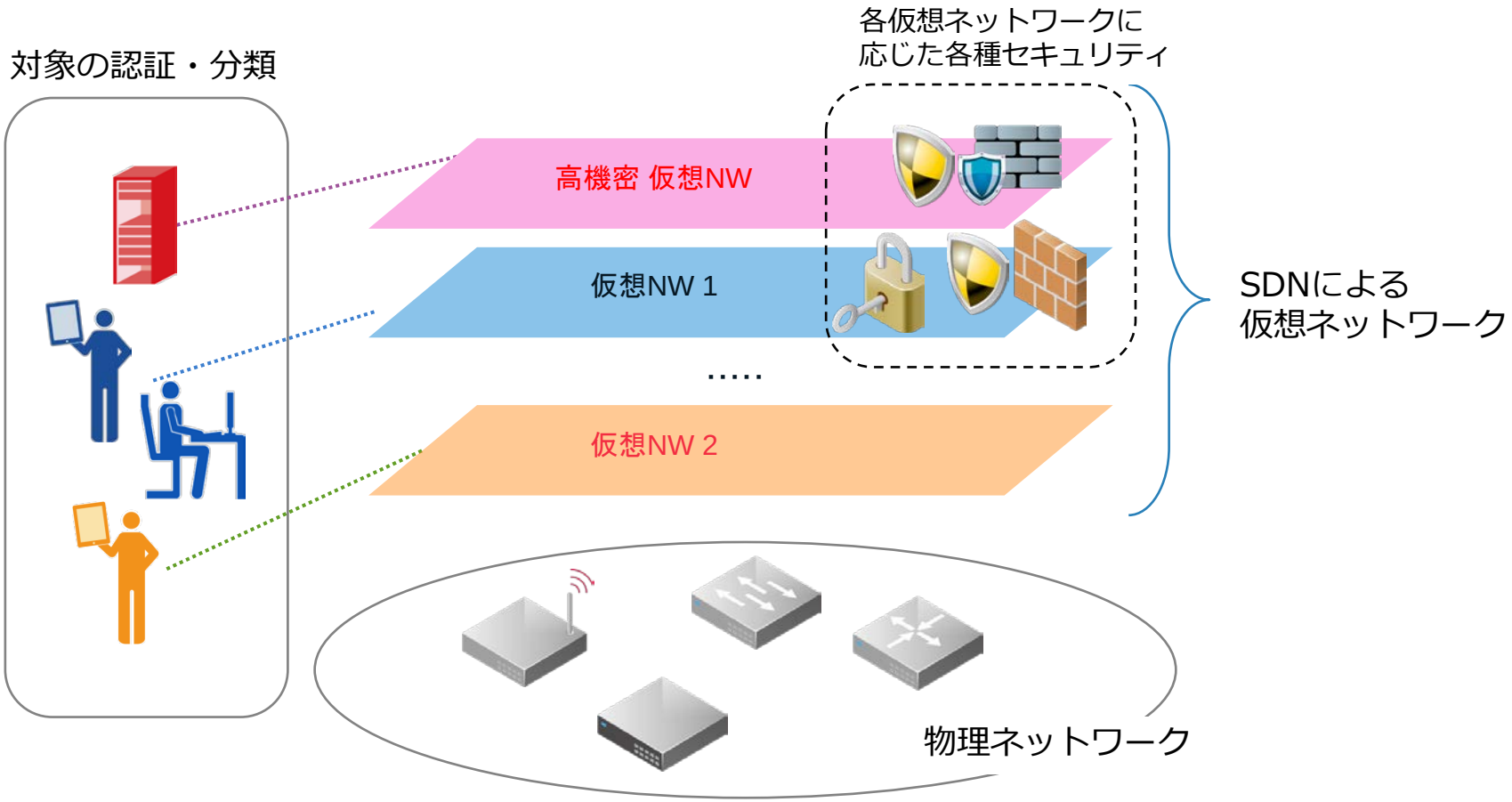
ITサービスとネットワークの融合

SDNのキーポイントは、アプリケーション・システム連携



SDNによる次世代セキュリティ

- 仮想ネットワーク分離による、ユーザ基点の新世代セキュアネットワークの構築
  - ユーザ・端末側だけではなく、ネットワーク側でのセキュリティ対策と連携
  - ユーザ・端末単位での細かな動的ネットワーク制御、問題箇所の局所化、拡散防止



SDNによる次世代セキュリティ

標的型サイバー攻撃の各段階 (IPA※1による定義)

SDNによる次世代セキュリティ

ユーザメリット

1:初期潜入段階
(例：脆弱性を狙った攻撃)

2:攻撃基盤構築段階
(例：マルウェアの設置)

3:システム調査段階
(例：サーバへの不正侵入)

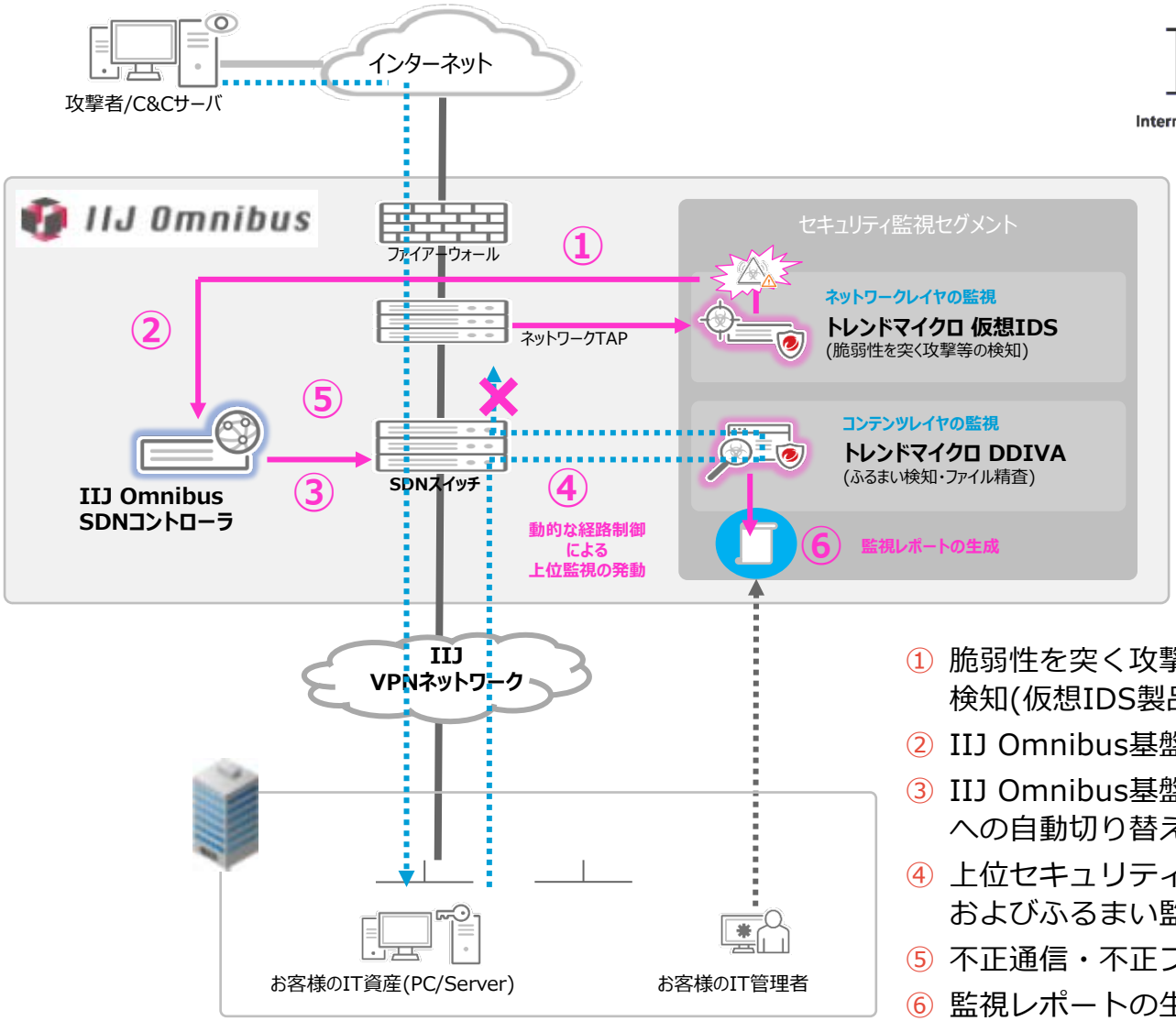
4:攻撃最終目的遂行段階(例：顧客情報奪取)

- 当該通信の自動遮断
- 感染端末の自動隔離
- C&C通信の自動遮断
- 疑わしい通信の自動監視(ログ取得等)
- 不正通信の自動遮断

- 被害範囲の特定とセキュリティリスクの最小化
- セキュリティ運用レベルの均一化と運用人員の削減
- ITサービスの維持・継続とビジネスリスクの排除

※1 IPA：独立行政法人情報処理推進機構
「新しいタイプの攻撃」より引用

トレンドマイクロ様との共同実証実験



Internet Initiative Japan

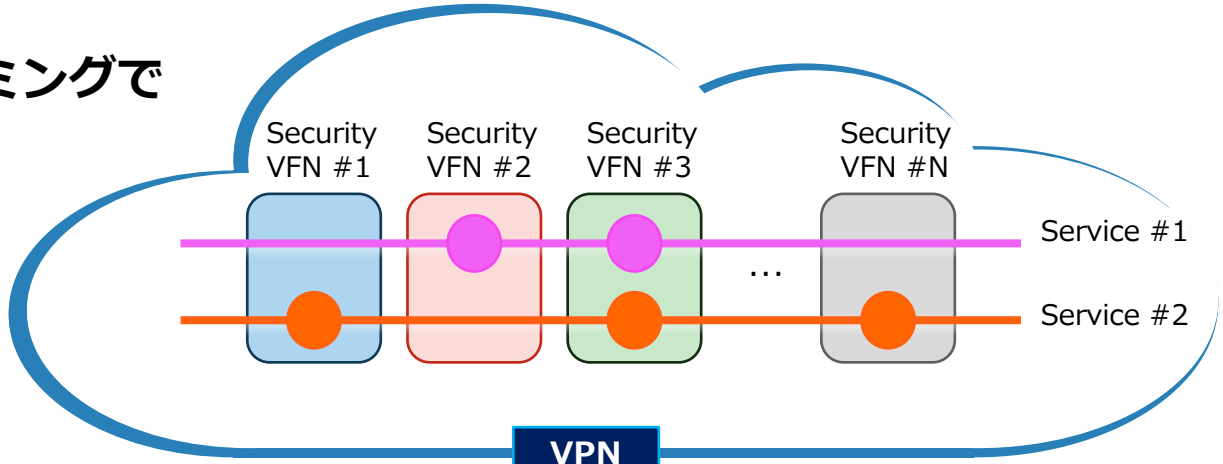
TREND MICRO
Securing Your Journey to the Cloud

① 脆弱性を突く攻撃をネットワークセキュリティ製品で検知(仮想IDS製品)
② IIJ Omnibus基盤への検知情報の通知
③ IIJ Omnibus基盤の動的変更と上位セキュリティ監視への自動切り替え
④ 上位セキュリティコンポーネントによるファイル精査およびふるまい監視(DDIVA)
⑤ 不正通信・不正ファイルの検出後のブロック
⑥ 監視レポートの生成

実証実験で目指すところ

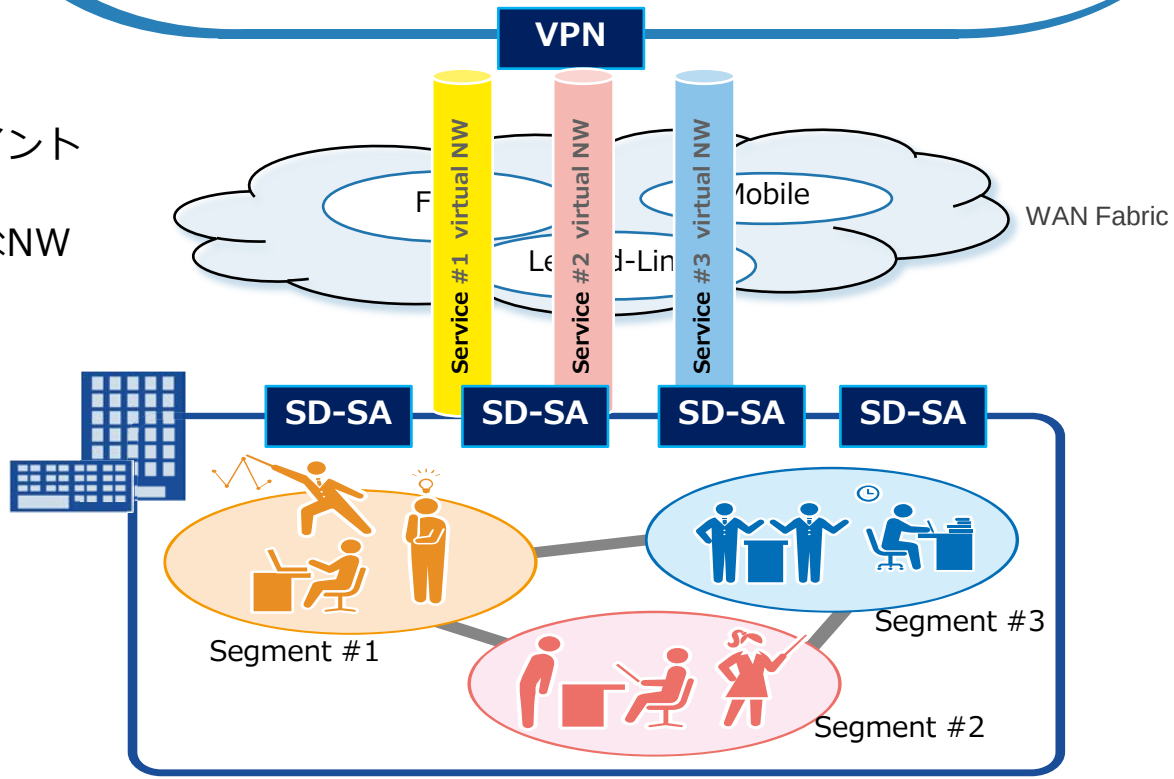
必要なところに必要なタイミングで自動配置

- フィルタ、IDS/IPS、DI 等
- コストを抑える



面で守るセキュリティ

- 企業ネットワークの様々なポイントに様々な脅威検知機能を配置
- 脅威検知をトリガにした動的なNW制御



第4部: 次世代セキュリティ まとめ

- SDN と NFV 技術で、面で守るセキュリティを実現
  - ユーザ基点のセキュアネットワークを構築

- IIJ Omnibus でのSDN基盤と、トレンドマイクロのVNF製品群を用いた実証実験

IIJ
Internet Initiative Japan

TREND MICRO™
Securing Your Journey to the Cloud

第5部
妄想の先に

続・理想のネットワーク

- **（再掲）個々の「誰」にポリシーを設定するのは面倒**
  - 管理対象のグループ化 → 仮想ネットワーク
- **「グループ」は仮想ネットワークである必要はない**
  - 同じ仮想ネットワークの別の人とL2通信することはない（だろう）
  - プリンタの自動探索ぐらい？
- **個人が複数のグループに属することを表現したい**
  - ネットワークアドレスでまとめることはできない
  - 1人1VLAN（≠ 802.11q）
  - OpenFlow + VXLAN (または MPLS）なら制御可能
- **フラットなアドレス空間（通し番号）でよい**
  - さらに考えると、IP アドレスは不要かも
  - 全員 10.0.0.1
  - スイッチでパケット書き換え
- **オンプレにもVNF**
  - 実証実験のVNFをオンプレに設置
  - SEILルータやホワイトボックススイッチ上のVM

今後の Omnibus SD-LAN（未定）

- **アクセス制御 （≠ ファイアウォール）**
  - 通信先 IP アドレス
- **認証方法の追加**
  - ロケーション、スケジュール
- **ゲスト用仮想ネットワーク**
- **機器ベンダとの協力強化**

IIJ Internet Initiative Japan

ご静聴ありがとうございました

Ongoing Innovation