古くて新しく活用され始めたセキュアなプロトコル ＨＩＰ！

セキュアなプロトコルHIPを利用するIDN(Identity-Defined Networking)とは?

～クローキング＆マイクロセグメンテーション～

Terilogy　/Takuma Miki

今日お伝えしたい事

＜自己紹介＞

名前：　御木拓真

所属：（株）テリロジー（今年で30周年のIT商社）

仕事内容：ニッチ・レアな要素技術持った製品を日本で展開するプロダクトマーケティングセールス

これまで：BAS・Radius・PPPoE・DPI・パケトキャプチャー・最近はICS/OT分野も

そして今日のHIP （Host Identity Protocol）を日本で広めようと・・・

今日お伝えしたい事

日本でも
HIPプロトコルを
使おう！！！

HIP （Host Identity Protocol）

×

Identity-Defined Networking（IDN）

ヒップ？

エイチアイピー？

HIPというプロトコル知っていますか？

独自プロトコル？

一覧 [編集]

10進数	16進法	略称	プロトコル	規格
0	0x00	HOPOPT	IPv6 Hop-by-Hop Option	RFC 2460
1	0x01	ICMP	Internet Control Message Protocol	RFC 792
2	0x02	IGMP	Internet Group Management Protocol	RFC 1112
3	0x03	GGP	Gateway-to-Gateway Protocol	RFC 823
4	0x04	IP-in-IP	IP in IP (encapsulation)	RFC 2003
5	0x05	ST	Internet Stream Protocol	RFC 1190, RFC 1819
6	0x06	TCP	Transmission Control Protocol	RFC 793
7	0x07	CBT	Core-based trees	RFC 2189
8	0x08	EGP	Exterior Gateway Protocol	RFC 888
9	0x09	IGP	Interior Gateway Protocol (any private interior gateway (used by Cisco for their IGRP))	
10	0x0A	BBN-RCC-MON	BBN RCC Monitoring	
11	0x0B	NVP-II	Network Voice Protocol	
12	0x0C	PUP	Xerox PUP	
13	0x0D	ARGUS	ARGUS	
14	0x0E	EMCON	EMCON	
138	0x8A	manet	MANET Protocols	RFC 5498
139	0x8B	HIP	Host Identity Protocol	RFC 5201
140	0x8C	Shim6	Site Multihoming by IPv6 Intermediation	RFC 5533
141	0x8D	WESP	Wrapped Encapsulating Security Payload	RFC 5840
142	0x8E	ROHC	Robust Header Compression	RFC 5856
143-252	0x8F-0xFC	UNASSIGNED		
253-254	0xFD-0xFE	Use for experimentation and testing		RFC 3692
255	0xFF	Reserved.		

これです！

出典: フリー百科事典『ウィキペディア（Wikipedia）』：プロトコル番号一覧

簡単に言うと・・・

Q:HIPとは？？？

A:セキュリティを考慮して作られたプロトコル

えっ！TCP/IPは？

TCP/IPは安全でない？？

TCP/IPプロトコルにおける課題

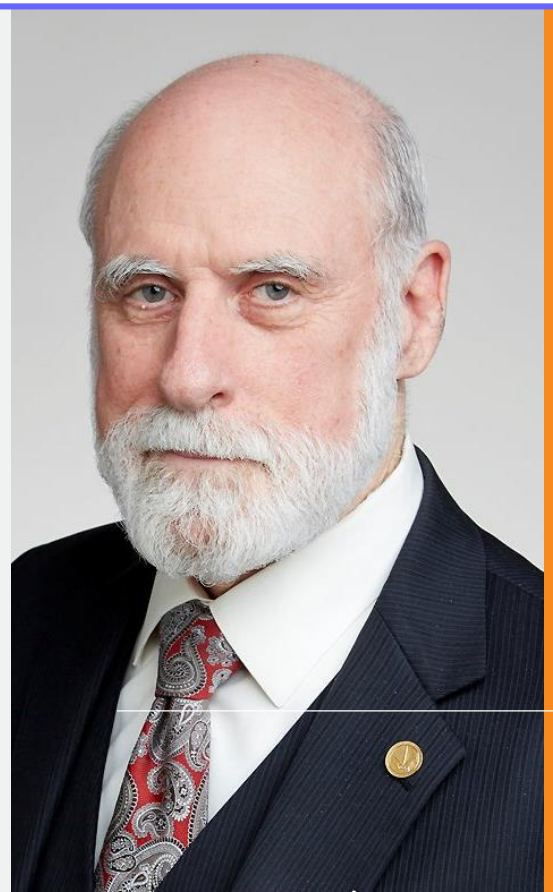
TCP / IPは、セキュリティやモビリティではなく、接続性のためだけに設計されています・・・

この方をご存知でしょうか？
HIPについて語っています！

EVERYTHING USES TCP/IP

BUT TCP/IP IS NOT

✕ Private	✕ Secure
✕ Mobile	✕ Simple



「もし時間を遡ることが出来れば、TCPの創生時に信頼できる認証とモビリティについてより良い仕事が出来ただろう。ただ当時、HIPというイノベイティブな考えは全く思いつかなかった」
byインターネットの父

VINT CERF
Co-Creator of the Internet & TCP/IP

HIP （Host Identity Protocol）の歴史は・・・・

1999年：米国海軍が”HIP”を考案

2004年：IETF内でHIPのWorking Group組織

：ボーイングR&DのDavid Mattesも参加

2005年：ボーイングプロジェクト開始。

⇒新型機７７７の開発の際に使用。プロジェクト状況に応じて柔軟に

ネットワークを変更

2015年4月：IETF（ Internet Engineering Task Force）でHIPが承認される

2015年10月：HIPを利用した商用製品をリリース

HIP（Host Identity Protocol）とは・・・・

・ID /ロケータの分離 をコンセプトにしたプロトコル！

：IDとLocatorを同時に持つIPアドレスには限界がある！！！　⇒**IDベースの通信へ**

：識別子を2048bit の RSA 公開鍵を使って強力に暗号化して、ユニークなIDとして識別

：IDを識別子、認証し、ホワイトリストに登録されたIDの相手のみと通信を実施

：ネットワークとして、拒否（DoS）攻撃や中間者攻撃にも耐性あり！

・HIPでセッションを張った後は、IPsec同等の暗号化（AES-256）で暗号化通信

TCPは繋げるを優先・・・　HIPはセキュリティを優先！

Internet 2.0 –
“Network everything”

アプリケーション (L5-L7)	IP Address: Port
トランスポート (L4)	IP Address: Port
ネットワーク (L2-L3)	IP Address
物理リンク (L1)	MAC address

UNTRUSTED
“まずは繋ぐ，⇒　そして認証＆許可！”

セキュアに,モビリティ、信頼されたNWへ

Internet 3.0 –
“Network ONLY CRYPTO-IDENTIFIED things”

アプリケーション（L5-L7）	**Host Identity Tag**: Port
トランスポート（L4）	**Host Identity Tag**: Port
Host Identity（L3.5）	**Host Identity Protocol (HIP)**
ネットワーク（L2-L3）	IP Address
物理リンク（L1）	MAC address

TRUSTED
“まずは認証＆許可　⇒　そして暗号化　⇒　繋ぐ”

では、このセキュアな
HIPプロトコルを
使っている仕組みは？

“Identity Defined Networking”
（ＩＤＮ）

SDNではないです・・・

Identity Defined Networking/IDN
（SecureSDN）

なにが嬉しいの？

→ HIP による オーバレイNW＆ネットワーク分離 ＆ 暗号化通信

→ 簡単にセキュアネットワークを！※既存NW構成OK/IP重複OK!

→ オーケストレーション＝センター集中の一元管理

→ 容易なマイクロセグメントを実現　～守りたい重要な個所を～

→ VLAN/ACL/IPアドレス設計からの脱却　⇒IDを指定するだけ！

現在の堅牢なネットワークは、設計は、構築は、、、

セキュリティを気にしながら作られるネットワークは、手間で設定が面倒である

頑張る

ルータ＆ファイヤーウォールで頑張る

```
interface gigabitethernet 0/3
        nameif dmz
        security-level 50
        ip address 192.168.2.1 255.255.255.0
        no shutdown
same-security-traffic permit inter-interface
route outside 0 0 209.165.201.1 1
nat(dept1) 1 10.1.1.0 255.255.255.0
nat(dept2) 1 10.1.2.0 255.255.255.0
router rip
        network 10.0.0.0
        default information originate
        version 2
ssh 209.165.200.225 255.255.255.255 outside
logging trap 5
```

課題

Different:
- IP/DNS Namespaces
- Security Controls
- Networking Context
- Workloads
- Address-Defined

人日工数

VLAN職人によるコンフィグ作業

```
Router>enable
Router>#configure terminal
Router(config)#hostname CORP
ISP(config)#interface serial 0/0/0
CORP(config-if)#description link to ISP
CORP(config-if)#ip address 192.31.7.6 255.255.255.252
CORP(config-if)#no shutdown
CORP(config)#interface fastethernet 0/1
CORP(config-if)#description link to 3560 Switch
CORP(config-if)#ip address 172.31.1.5 255.255.255.252
CORP(config-if)#no shutdown
```

課題

Different:
- IP/DNS Namespaces
- Security Controls
- Networking Context
- Networks
  - Internet
  - MPLS
  - WiFi
  - Cellular

面倒

ACLを追加・変更・面倒・・

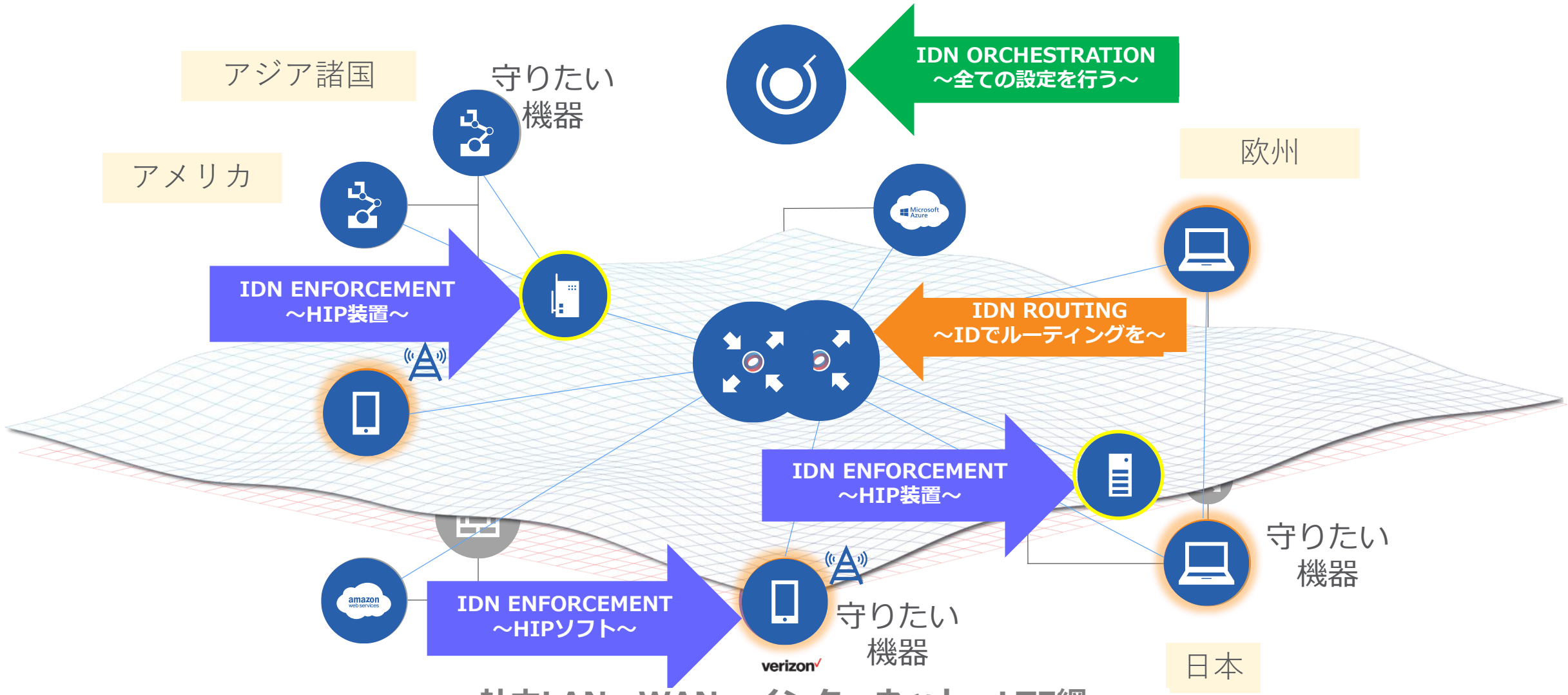
```
device(config)# ip access-list standard Net1
device(config-std-nacl-Net1)# deny host 10.157.22.26
device(config-std-nacl-Net1)# deny 10.157.29.12
device(config-std-nacl-Net1)# deny host IPHost1
device(config-std-nacl-Net1)# permit any
device(config-std-nacl-Net1)# exit
device(config)# int eth 1/1
device(config-if-e10000-1/1)# ip access-group Net1 in
```

VPNのルールをガリガリ・・・

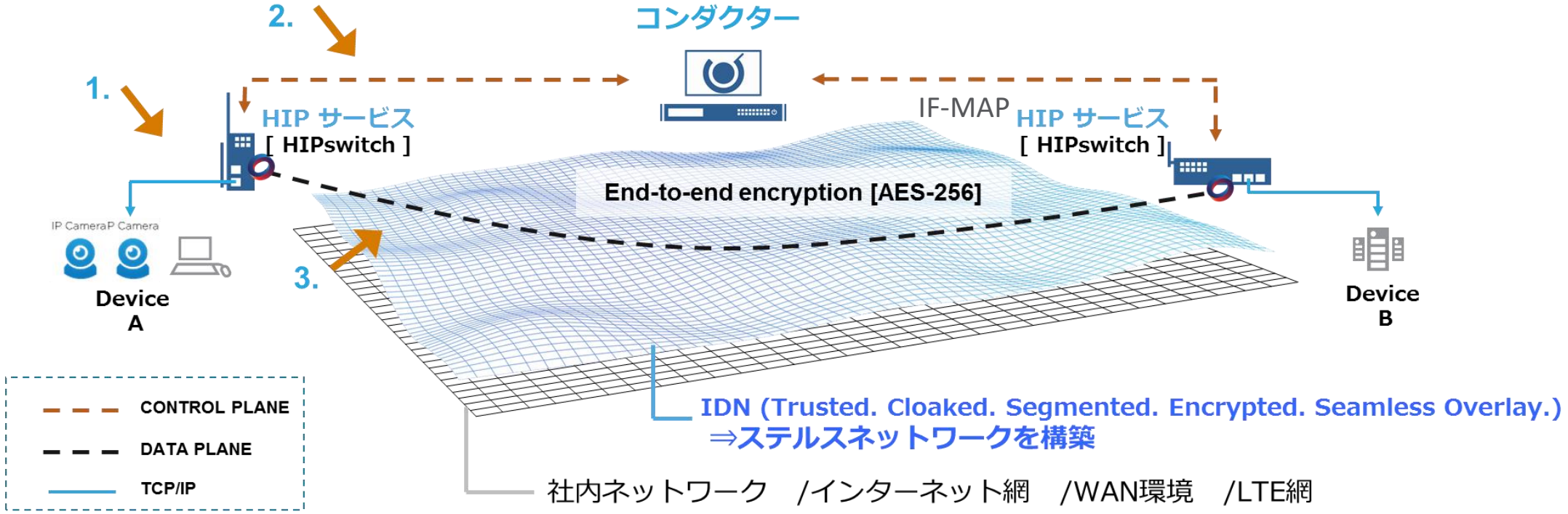
作業・作業・作業

Identity Defined Networking

～いつでも、どこでも、容易にIDベースで管理者が定めたデバイスだけの セキュアNWを実現～



Identity-Defined Networking (IDN)
今後の解決方法 = 複雑なネットワークから解放！



1. HIPサービスの配下で保護されたIoTデバイスの設定

2. 認証可能なアイデンティティに基づく構成とポリシー管理を簡単に推進します

3. HIP サービスは、互いに認証・証明書ベースのカプセル化セキュリティペイロード（ESP）で保護されたトンネルを構築します。

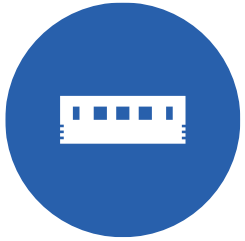
Identity Defined Networking platform

～容易にセキュアネットワーク接続・ネットワークセグメンテーション・NW管理を実現～

オーケストレーションエンジン

設定・変更を一元的に

IDN ORCHESTRATION



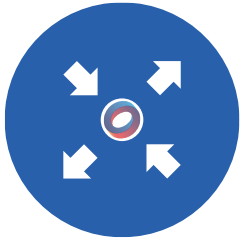
HIPデバイス

&

HIPクライアントソフト

各デバイス/セグメントに配備

IDN ENFORCEMENT



IDルータ

復号化せずにプライベートまたは非ルーティングエンドポイント間のピアツーピア暗号化接続を許可します

IDN ROUTING

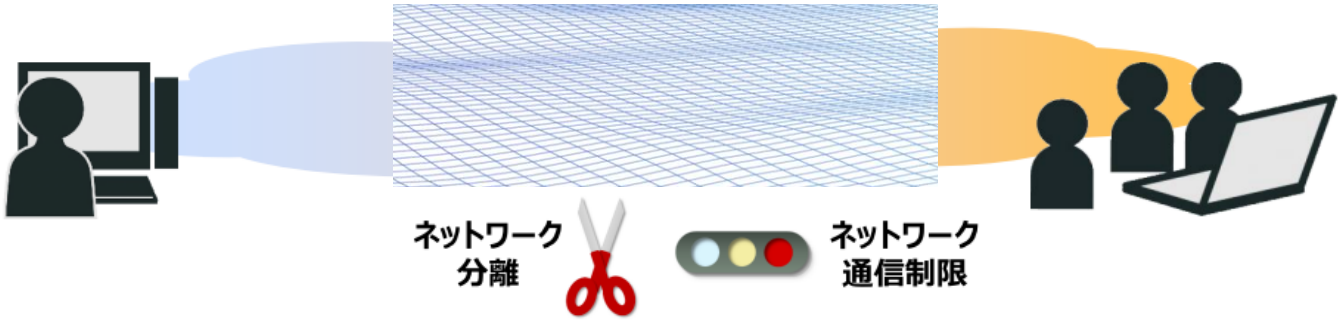
HIP × IDN

こんな使い方どうでしょう

こんなシーンで簡単なセキュアネットワークのご利用！

～NW分離・暗号化通信を必要～

✓ セキュリティ管理のためにセキュリティレベルの異なるネットワークを分離して通信を制限する



✓ インターネットとの接続

✓ 制御システムネットワーク接続

✓ 企業間接続（B2B接続、保守用途）

✓ 研究開発ネットワーク（最重要機密）

✓ 本番環境と開発環境の接続

✓ 機密情報管理ネットワーク（大量機密）

実際の利用ケース①

米国です！

◆マイクロセグメンテーションとHIPトンネルによるセキュアNW接続

お悩み

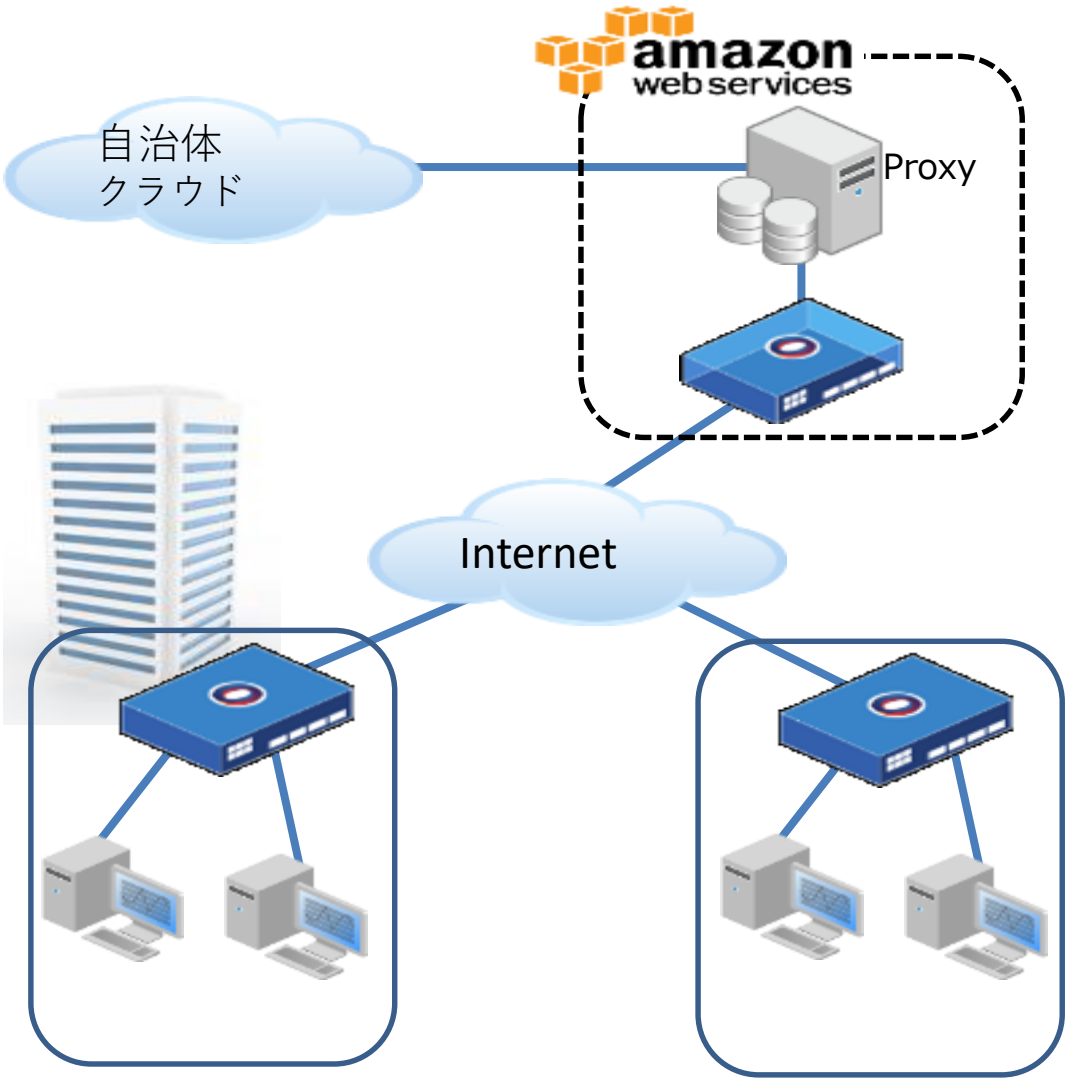
- 自治体システムの運営を委託されているが、自治体側と自社の異なるセキュリティポリシーを共存させる必要がある

メリット

- マイクロセグメンテーションとホワイトリスト設定による通信端末の限定

ポイント

- 既存NWを使用したまま、NW分離の実現
- AWS環境を利用したサーバレス構成



実際の利用ケース②

米国です！

◆ステルス化とLTE網によるガントリークレーンの制御と集中管理

お悩み

- ガントリークレーンへの貨物データの配信や制御の為、個別にUTM及びWifi網を設置していたが運用コストが高い上に個別の設定ミスによる事故を心配

メリット

- UTMからHIPスイッチへ置き換え
- 通信先を限定へ

ポイント

- マイクロセグメンテーション化による安全性の向上とIDNによる集中管理による運用コスト低減と設定ミス防止

実際の利用ケース③

米国です！

◆マイクロセグメンテーションによるBAのセキュア化

お悩み

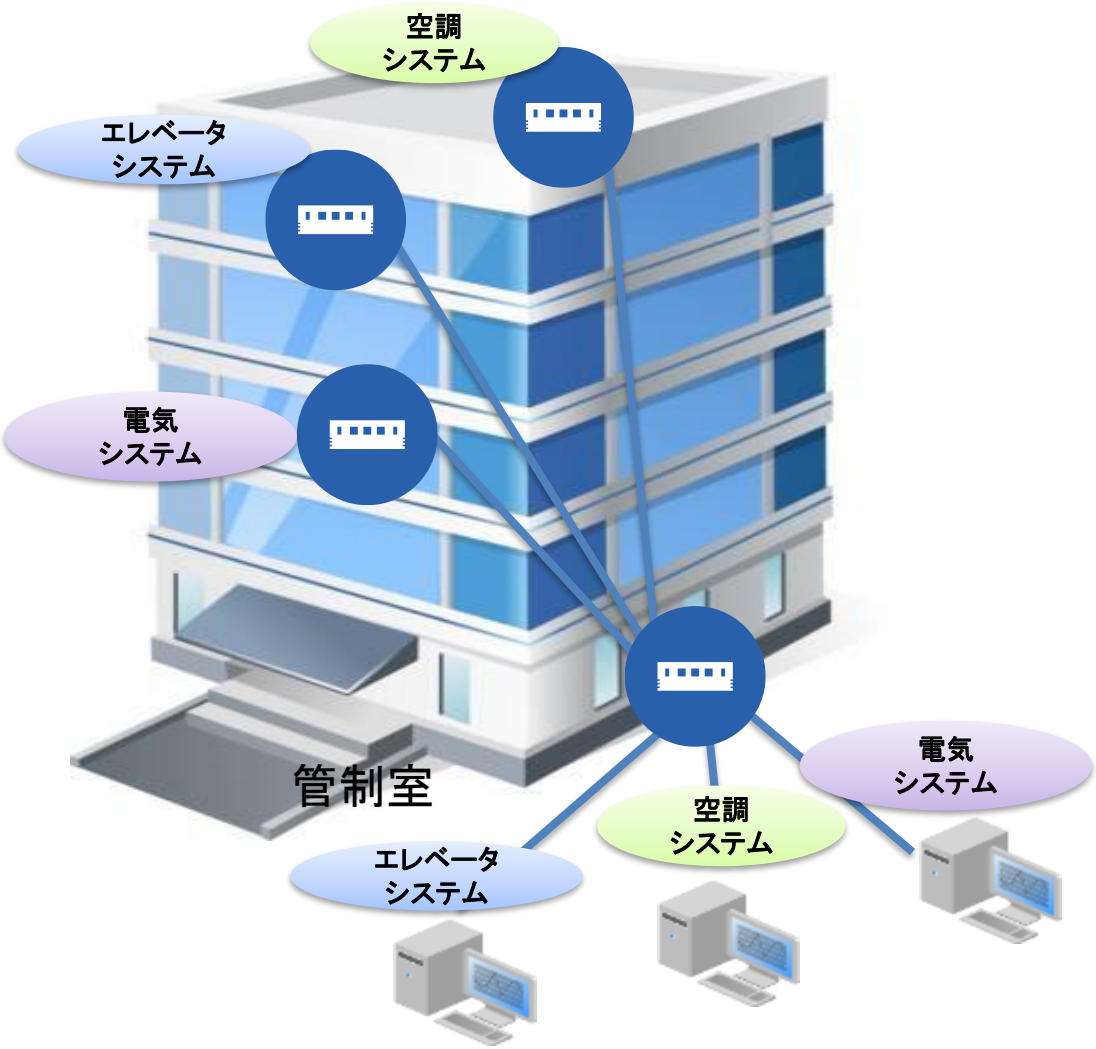
- ビル内のネットワーク（空調/エレベータ/電気等）はL2フラットで構成されており、攻撃を受けた際にビル全体に被害が及ぶ危険性がある。

メリット

- 既存NWのシステム前段にHIPSwitchを設置するだけで、各システムごとにマイクロセグメンテーション化。また、外部から各システムへの攻撃もステルス化により抑制。

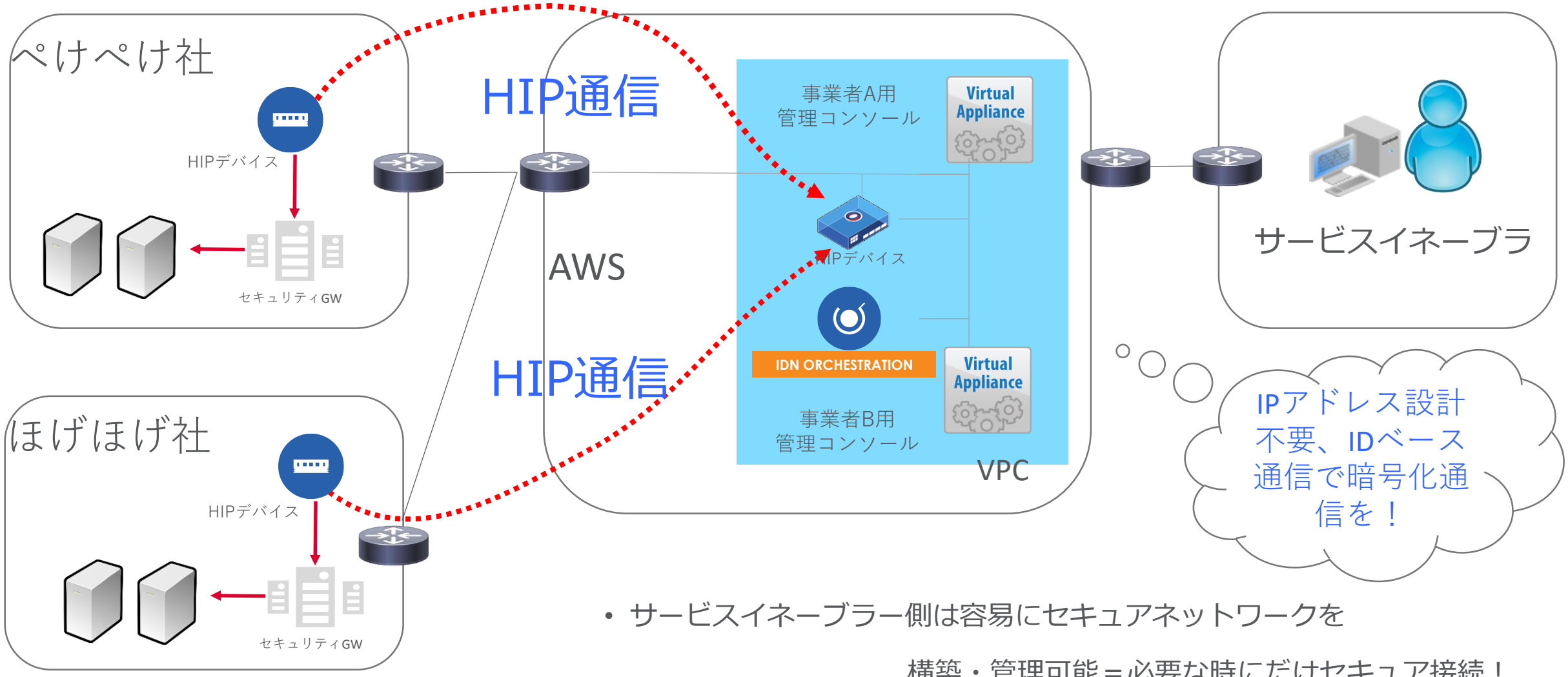
ポイント

- NW上に挟むだけでマイクロセグメンテーションが可能許可したデバイス間の通信のみ疎通が可能なので、外部攻撃による内部探索や感染拡大を抑制可能



私たちは、国内で
最近こんなことやって
みました！

クラウドセキュリティサービスを容易にセキュアに提供！



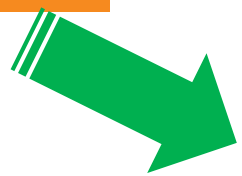
- サービスイネーブラー側は容易にセキュアネットワークを
  構築・管理可能＝必要な時にだけセキュア接続！
- 脆弱性診断を行う管理サーバをAWS上で動かし複数の顧客にサービス提供
- 顧客にはセキュリティGWを送付

ハイブリット環境でセキュアなPeer to Peer！

「オンプレDC　と　AWS　と　Azureをつなぐ！」

「NW設計意識せずにGUIでクリックするだけで」

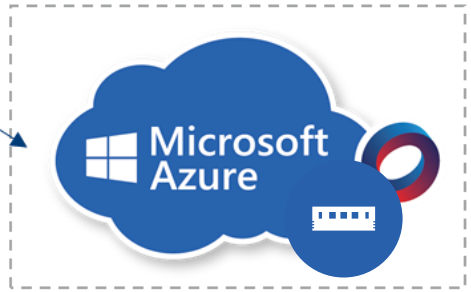
IDN ORCHESTRATION



Test stage/DevOps

Production/DevOps

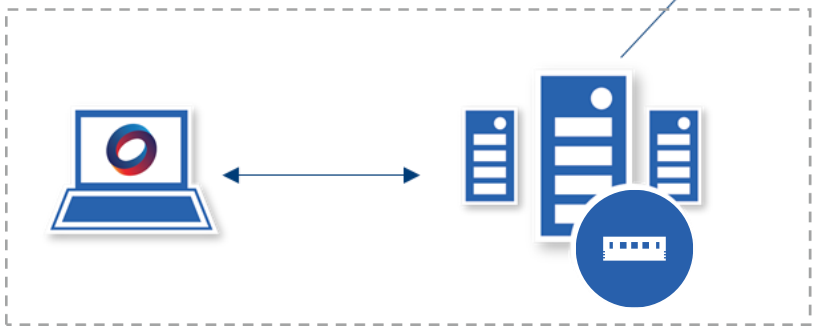
Production/DevOps



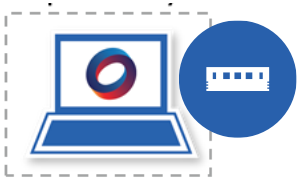
On-demand
per instance peering

Micro-services peering,
integration, and
workload migration

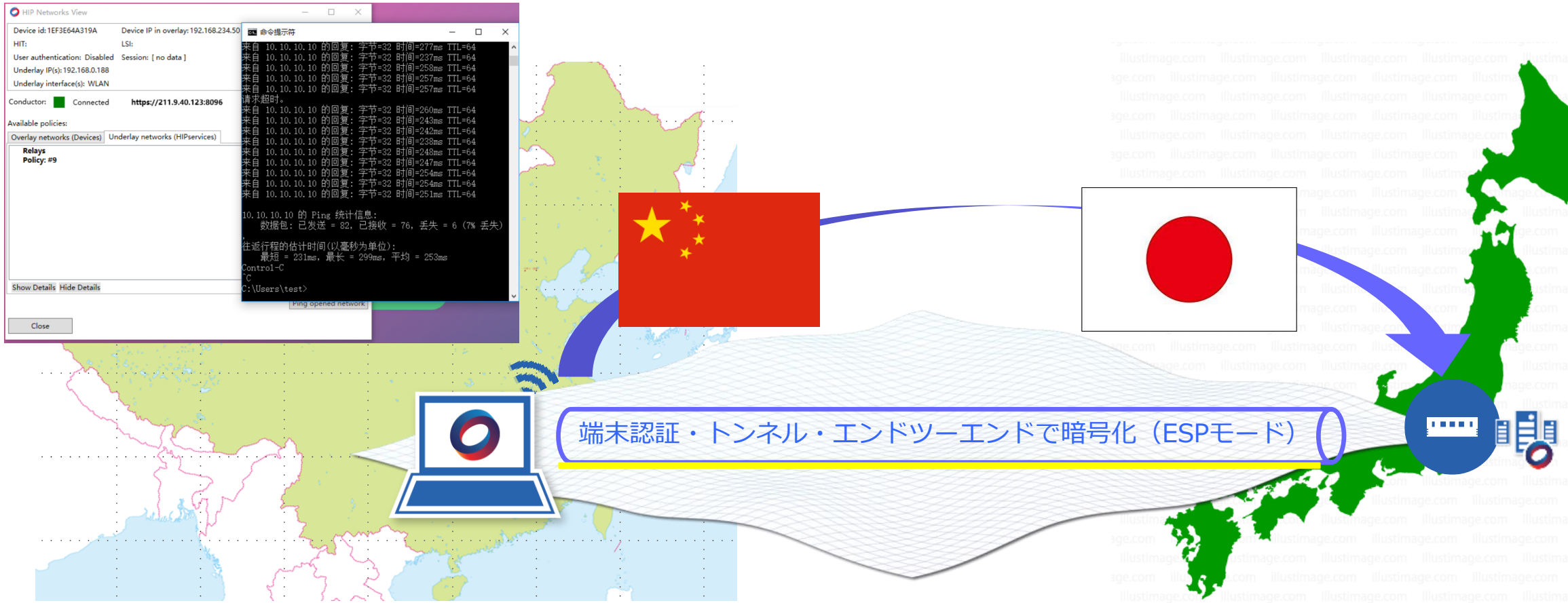
オンプレDC　DevOps



リモート接続/DevOps



諸外国とHIPを利用してPeer to Peer！



- ぜひ今ご利用のTCP/IPから、、、

  必要な箇所にはHIP（Host Identity Potocol）をお使いください！

- IPアドレス設計・VLAN管理・ACL設定・VPNから新たなステージへ

  容易なセキュアネットワークをお試し下さい！

ぜひ、会場で私までお声がけください！

Fin.

詳細及びご質問は下記までご連絡を

tmiki@terilogy.com　/　in 九段下